

Enterprise Architecture Document

Stakeholders

Rol	Naam
Enterprise Data Architect	Jean-Michel COGNIAUX (JMC)
	Alain PERSOONS (APE)
Security Architect	Sébastien BERNARD (SBE)
	Costas SIMATOS (CSI)
Business Analyst	Laureen MADEJ (LMA)
	Alexia WINANDY (AWI)
Functional Analyst	Philippe EVRARD (PHE)
	Maxime MICHEZ (MMI)
	Arnaud PIRLOT (API)
Technisch analist	Amory SCHOONBROODT (ASC)
	Olivier BLANPAIN (OBL)
Project Manager	Aurélie HERKENNE (AHE)
Data Privacy Officer	Francis OUAAL (FOA)

Herziening van de inhoud

Elke nieuwe versie van het document moet worden opgenomen in de onderstaande tabel. Elke versie moet een status toegewezen krijgen: "Creation", "Update", "Final draft", "Review", "Approval", "Published".

Versie	Datum	Wie	Status	Wijzigingen
0.1	10/05/2022	JMC	Draft	Initiëring van het document
0.2	27/06/2023	JMC	Update	Integratie van de opmerkingen van de belanghebbenden

Inhoud

1	Referenties.....	4
2	Context	4
3	Doelstellingen van het document	6
3.1	Verwijzing naar Archimate	6
3.2	Verwijzing naar TOGAF	7
3.3	Logische benadering.....	8
4	Omschrijving	9
5	Beperkingen.....	11
6	Werkhypothesen.....	11
7	Bedrijfsbehoeften	13
8	Evaluatie van de risico's	15
9	Vereisten.....	17
9.1	Bedrijfsvereisten	17
9.2	Functionele vereisten.....	21
9.3	Niet-functionele vereisten.....	24
9.4	Technische vereisten.....	27
9.5	Beveiligingsvereisten	31
9.6	Vereisten buiten het toepassingsgebied	34
10	Oplossing	38
10.1	Motivatiediagram	38
10.2	Bedrijfsarchitectuur (BusinessLayer)	44
10.3	Functionele toepassingsarchitectuur (Application Layer)	45
10.4	Technische architectuur (Technology Layer)	52
10.5	SWOT	53
10.5.1	SWOT Business.....	55
10.5.2	Technische SWOT	57
11	Bijlagen.....	61
11.1	Glossarium	61
11.2	Archimate-elementen	62
11.2.1	Business Architecture.....	62

11.2.2	Architecture Application	63
11.2.3	Architecture Technology	64

1 Referenties

	Documentnaam	Beschrijving	Auteur
REF01	Lijst van de use cases	Lijst van use cases per systeem, gebruikt als basis voor het analyseren van de risk assessments en het vaststellen van de verschillende requirements	NRB & Civadis
REF02	PROJECT NETVOTING_BE - Rapport deel 1	Studie over de mogelijkheid om online stemmen in België in te voeren Deel 1 (ver. 4 december 2020)	Hoofdpromotor: Prof. Jean-Benoit Pilet (Université libre de Bruxelles) Promotoren: Prof. Bart Preneel (KU Leuven), Prof. Silvia Erzeel (Vrije Universiteit Brussel), Prof. Olivier Pereira (UCLouvain)
REF03	Functioneel schema van hybride stemmen		Civadis
REF04	CDC		Inrichtende macht
REF05	Website https://elections.fgov.be/	Officiële Belgische website	fgov

2 Context

Dit document is een vervolg op de interuniversitaire studie NETVOTING-BE (J.-B. Pilet et al., Étude sur la possibilité d'introduire le vote Internet en Belgique, elections.fgov.be, 2020).

Het onderwerp van deze studie was elektronisch stemmen in België. Ze is opgebouwd rond vier dimensies van het online stemmen:

- de IT-dimensie en de beveiliging van het stelsysteem
- de aanvaarding door burgers en overheden (sociaal-politieke dimensie)
- de organisatorische dimensie
- de wettelijke en regelgevende dimensie

De doelstellingen van de studie luiden als volgt:

- Een gedetailleerde inventaris opmaken van de ervaringen met online stemmen in vijf landen: Australië, Estland, Frankrijk, Noorwegen en Zwitserland.
- Nagaan in welke mate deze ervaringen kunnen worden omgezet naar België.

De NETVOTING-BE studie concludeerde als volgt: "Gezien de moeilijkheden die nog steeds verbonden zijn aan het stemmen via internet en die moeilijk te overwinnen blijven in een context van overheidsverkiezingen, bestudeert een aantal onderzoekers steeds actiever de mogelijkheid

om een aantrekkelijke tussenstap aan te bieden tussen het stemmen in een stembureau en het stemmen via internet. Bijvoorbeeld, in het geval van een stelsysteem per post met bepaalde online componenten, zou de kiezer toegang kunnen krijgen tot zijn of haar stembiljet via het internet, waardoor de vaak riskante logistiek van het verzenden van post naar de kiezer wordt vermeden, in het bijzonder voor kiezers die in het buitenland wonen. Het stembiljet (of een vereenvoudigde versie van het stembiljet met alleen de keuze van de kiezer als die via de computer wordt gemaakt) moet door de kiezer worden afgedrukt, ingevuld en naar een stembureau worden gestuurd. Deze strategie heeft het voordeel dat het probleem van de individuele controleerbaarheid de facto wordt opgelost: de kiezer kan er zeker van zijn dat zijn papieren stembiljet zijn stemintentie weergeeft".

3 Doelstellingen van het document

De doelstellingen van dit "Enterprise Architecture Document" zijn:

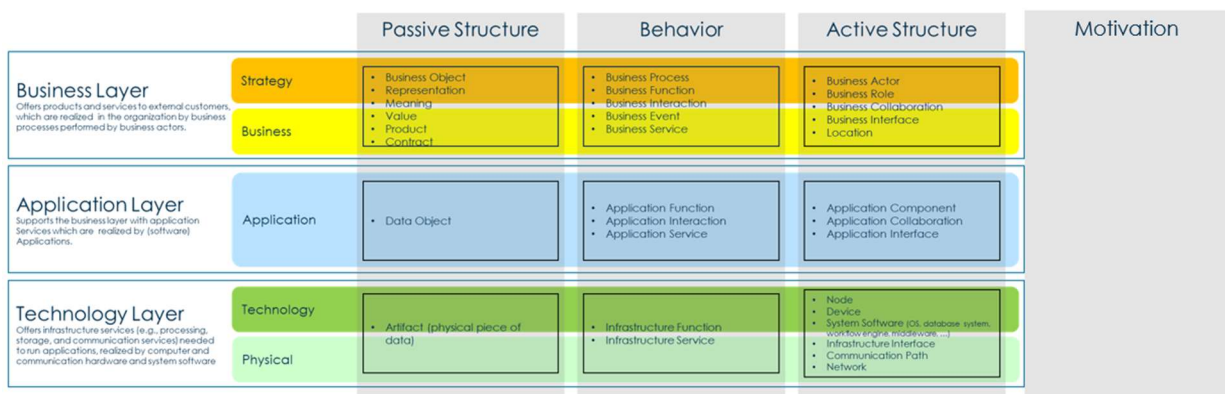
- De beslissing ondersteunen om de beste oplossing te implementeren, in lijn met de doelstellingen en naleving van de vereisten.
- De oplossing documenteren en beslissingen rationaliseren:
 - o Als basis dienen voor het schatten van de kosten van de oplossing
 - o Een overzicht op hoog niveau bieden van de oplossing in termen van bedrijfs-, toepassings- en technologische aspecten
 - o Dienen als input voor:
 - Opstellen van de SWOT-matrix
 - Identificeren van mogelijkheden voor volledig of gedeeltelijk hergebruik tussen verschillende systemen
 - "Solution Architecture Document: analyse en ontwerp van meer gedetailleerde zakelijke, functionele en technologische architecturen

Dit "Enterprise Architecture Document" beschrijft de behoeften en vereisten, evenals verschillende high-level architecturen die nuttig zijn voor het implementeren van de vraag.

Dit document behandelt bedrijfs-, toepassings- en technologische aspecten, inclusief context, risicoanalyse en informatiemodellen.

3.1 Verwijzing naar Archimate

Dit document verwijst naar de Archimate-modelleertaal en stelt architectuurartefacten voor in de volgende drie lagen: bedrijf, toepassing en technologie.



3.2 Verwijzing naar TOGAF

Dit document verwijst naar de concepten van Building Blocks: de ABB's.

Het "Open Group Architecture Framework", ook bekend onder het acroniem TOGAF, is een verzameling concepten en een industriestandaard op het gebied van IT-architecturen voor bedrijven.

Twee belangrijke elementen van het framework zijn de ABB's ("Architecture Building Blocks") en SBB's ("Solution Building Blocks").

Een "Building Block" is een verzameling functionaliteiten die zijn gedefinieerd om te voldoen aan de behoeften van de onderneming binnen een organisatie.

ABB → IN SCOPE van dit document "Enterprise Architecture Document"

- Definieren welke functionaliteiten er geïmplementeerd zullen worden
- Bedrijfsmatige, functionele en technologische vereisten
- De ontwikkeling van de SBB's sturen en leiden
- De ABB-specificaties omvatten minstens de volgende elementen:
 - o Fundamentele functionaliteiten en attributen, inclusief capaciteit, beveiliging en onderhoud, ...
 - o Interfaces: API's, gegevensformaten, protocollen, hardware-interfaces, normen, ...
 - o Bouwstenen afhankelijk van de vereiste functionaliteiten
 - o Relatie met entiteiten en bedrijfs-/organisatiebeleid

SBB → OUT of SCOPE van dit "Enterprise Architecture Document"

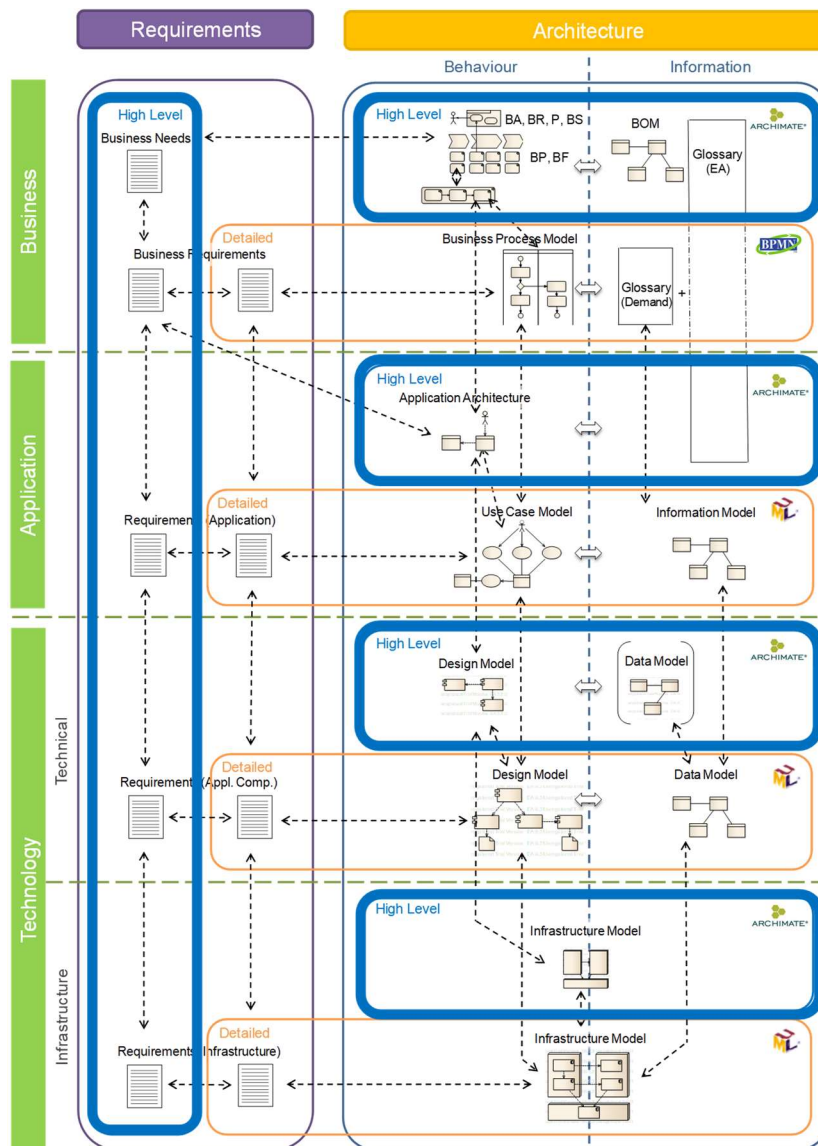
Dit wordt behandeld in het "Solution Architecture Document".

- Definieren welke hardware, software, editors, enz. de functionaliteit zullen implementeren
- De implementatie definiëren
- Tegemoetkomen aan de beperkingen die zijn geïdentificeerd in ABB
- De SBB-specificaties omvatten ten minste de volgende elementen:
 - o Specifieke functionaliteiten en eigenschappen
 - o Interfaces
 - o Integratie van SBB's in het IT-landschap en het operationele beleid
 - o Specificatie van gedeelde kenmerken binnen de totale IT-omgeving: beveiliging, locatie, schaalbaarheid, prestaties, configuraties, enz.
 - o Ontwerppilots en -beperkingen, inclusief fysieke architectuur

3.3 Logische benadering

Dit document respecteert ook de volgende logische benadering:

- Verzamelen van de bedrijfsbehoeften (Business Needs)
- Bepalen van de bedrijfsvereisten (BR - Business Requirements)
- Bepalen van de functionele vereisten (FR – Functional Requirements)
- Bepalen van de niet-functionele vereisten (NFR – Non Functional Requirements)
- Bepalen van de technische vereisten (TR – Technical Requirements)
- Bepalen van de veiligheidsvereisten (SEC – Security Requirements)
- Bepalen van de bedrijfsarchitecturen
- Bepalen van de logische architecturen
- Bepalen van de toepassingsarchitecturen
- Bepalen van de technologische architecturen



4 Omschrijving

Het project heeft betrekking op het uitvoeren van een studie over de functionele, budgettaire, technische en veiligheidsbeschrijving van de ontwikkeling van een online stelsysteem, evenals het onderhoud en de controle ervan, voor verkiezingen die in België door de federale overheid worden georganiseerd (d.w.z. voor Europese, federale en gewestelijke verkiezingen).

Het resultaat van dit werk belicht 3 verkiezingssystemen:

1. Hybride online stelsysteem
- ~~2. Volledig online stelsysteem~~
- ~~3. Kioskstelsysteem~~

Dit document behandelt alleen het hybride online stelsysteem. De volledig online en kiosksystemen worden behandeld in andere Enterprise Architecture Documents.

De klant wil een set specificaties voor het geval een van de oplossingen in de toekomst wordt geïmplementeerd:

1. De functionele vereisten
2. De vereisten op het vlak van beveiliging en cyberveiligheidselementen
3. De vereisten inzake integriteit, vertrouwelijkheid, verifieerbaarheid, transparantie en monitoring
- ~~4. Een realistisch tijdschema voor de ontwikkeling van dit systeem~~
- ~~5. Een raming van de globale kostprijs van de infrastructuur en de ontwikkeling, uitgesplitst per module (CAPEX + OPEX)~~
- ~~6. Een capaciteitsplan inzake middelen voor de implementatie~~
- ~~7. Een raming van de kosten voor onderhoud, audit en controle van de oplossingen (OPEX)~~

Alleen de punten 1, 2 en 3 zijn opgenomen in dit Enterprise Architecture Document. De andere punten worden in andere documenten behandeld.

De authenticatie die nodig is om toegang te krijgen tot het systeem vereist een CSAM-verbinding¹ (eID of ItsMe). Voor Belgen in het buitenland die geen geactiveerde identiteitskaart hebben, omvat de CSAM-authenticatie alternatieve authenticatiemethoden naast eID en ItsMe die van toepassing zijn. De implementatie van deze alternatieve authenticatiemethoden heeft geen impact op de software die zal worden gecreëerd en is enkel een kwestie van configuratie (bv. een tweede instantie voorzien voor dezelfde toepassing waardoor Belgen die geen gebruik kunnen maken van eID of ItsMe zich kunnen authenticeren).

In elk van de drie verkiezingssystemen wordt de status van de stem gecontroleerd en geeft een bevestigingsbericht aan of de stem al dan niet in aanmerking is genomen. In het geval van het hybride systeem gebruikt de kiezer een "K"-verificatiecode die overeenkomt met het betreffende stembiljet.

¹ De CSAM-authenticatie omvat alternatieve authenticatiemethoden met hetzelfde zekerheidsniveau die onder andere van toepassing zijn voor Belgen in het buitenland.

Een dubbele verificatie van stemmen wordt vermeld in het interuniversitaire project Netvoting-be (J.-B. Pilet et al., Étude sur la possibilité d'introduire le vote Internet en Belgique, elections.fgov.be, 2020). Deze dubbele verificatie houdt rekening met het feit dat de stem is geregistreerd en voorziet ook in de mogelijkheid om de inhoud van de stem te verifiëren. De in de studie genoemde mogelijkheid om de inhoud van de stem te controleren, is in deze analyse niet overgenomen om praktische redenen die verband houden met de uitvoering, de haalbaarheid en het stemgeheim.

5 Beperkingen

	Datum	Wie	Beschrijving
CTR01	23/06/23	PHE	Het implementeren van elke oplossing vereist wijzigingen in de huidige wetgeving. Dit vereist a priori een politiek akkoord.
CTR02	23/06/23	PHE	Naleving van de verkiezingsagenda.
CTR03	23/06/23	APE	Het systeem kan niet worden gehost in de cloud: de bronnen en de applicatie, zowel in de ontwikkelings- als in de productiefase.

6 Werkhypothesen

	Datum	Wie	Beschrijving
HYP01	01/06/2023	JMC	<p>Het stelsysteem is bedoeld voor verkiezingen georganiseerd door de federale overheid. De betrokken niveaus zijn:</p> <ul style="list-style-type: none">• Europees (Europees Parlement)• Federaal (Kamer van Volksvertegenwoordigers)• Gewestelijk (Waals, Vlaams en Brussels Parlement en Raad van de Duitstalige Gemeenschap) <p>De provinciale en gemeentelijke verkiezingen vallen niet onder deze studie.</p>
HYP02	01/06/2023	JMC	<p>De hybride systeembenadering IS een traditioneel papieren stelsysteem met een paar elektronische componenten:</p> <ul style="list-style-type: none">• Bewerking en verzending van de stembiljetten• Verificatie van de inaanmerkingneming van de stemmen van de kiezers• Ontvangst van de stemmen per post <p>De hybride systeembenadering IS GEEN elektronisch stelsysteem met een paar traditionele componenten:</p> <ul style="list-style-type: none">• Papieren stembiljetten• Fysieke ontvangst van papieren stembiljetten• Stemopneming en manuele invoer van de stemmen
HYP03	01/06/2023	JMC	<p>Het hybride systeem IS een module die onafhankelijk is van de andere verkiezingsmodules en de volgende functies ondersteunt:</p> <ul style="list-style-type: none">• Verzending van digitale stembiljetten naar de kiezers• Verificatie van de inaanmerkingneming van de stemmen van de kiezers <p>Deze module ontvangt informatie (gegevensbestandoverdracht) van verschillende stembeheermodules en ondersteunt de volgende functies:</p>

			<ul style="list-style-type: none"> • Opstelling van de kieslijsten • Opstelling van de partij- en kandidatenlijsten • Ontvangst van de samenstelling van de bureaus • Ontvangst van niet-aanwezigheden en weigeringen om deel te nemen bij de ontvangst- en stemopnemingsbureaus • Telling van de omslagen • Invoer van de stemmen • Verificatie van de stemmentelling • Opstelling van het proces-verbaal (samenstelling van de bureaus, details van de operaties zoals eerste telling, enz.) <p>Het hybride systeem IS GEEN oplossing die alle functionaliteiten bevat die nodig zijn voor het stemmen, geïntegreerd met de verschillende modules voor stembeheer, en die de volgende functies ondersteunt:</p> <ul style="list-style-type: none"> • Opstelling van de kieslijsten • Opstelling van de partij- en kandidatenlijsten
HYP04	02/06/2023	JMC	<p>Een in persoon uitgebrachte stem heeft voorrang op alle andere stemmen.</p> <p>Als de kiezer meerdere stelsystemen gebruikt, is de in persoon uitgebrachte stem de enige die in aanmerking wordt genomen, ongeacht of de kiezer stemt met een geldig, verdacht of blanco/ongeldig stembiljet.</p>

7 Bedrijfsbehoeften

Business Needs [BN].

De bedrijfsbehoefte is de uitdrukking van een wens, verlangen, probleem of frustratie om gestelde doelen of doelstellingen te bereiken. De zakelijke behoefte is de reden "waarom" het project is gestart (algemene doelstelling).

BN001 Het/de eigen stembiljet(ten) via zelfbediening verkrijgen

De kiezer maakt verbinding met de server waarop de oplossing staat via een beveiligd webnetwerk.

De kiezer logt in op het systeem om toegang te krijgen tot zijn stembiljet.

De kiezer drukt zijn stembiljet(ten) en etiketten af om de dubbele omslagen naar de hoofdbureaus van de kieskringen te sturen.

BN002 Vooraf stemmen

Kiezers stemmen met het/de stembiljet(ten) dat/die ze hebben afgedrukt.

De kiezer noteert de controlecode "K" op het/de stembiljet(ten).

De kiezer verstuurt zijn ingevulde stembiljet(ten) in gelabelde dubbele omslagen per post

BN003 Tellen van de vooraf uitgebrachte stemmen op de dag van de stemming

De stemopnemings-/ontvangstbureaus ontvangen de dubbele omslagen van de stemmen uitgebracht in België en de stemmen uitgebracht door Belgen in het buitenland.

De stemopneming van het hybride stelsysteem gebeurt na die van de stemming in persoon.

De leden van de ontvangst-/stemopnemingsbureaus voeren de stemmen in het systeem in.

BN004 Controleren of er rekening is gehouden met de stem(men) in zelfbediening

De kiezer maakt verbinding met de server waarop de oplossing staat via een beveiligd webnetwerk.

Kiezers controleren of hun stem(men) in aanmerking zijn genomen door hun verificatiecode "K" in te voeren.

BN005 Doorlichten van het stelsysteem

De inrichtende macht moet het systeem kunnen controleren (interne en externe audits) tijdens en buiten verkiezingsperioden. Het moet ook de controlepunten en tolerantiedrempels definiëren en ervoor zorgen dat het systeem correct en veilig werkt.

BN006 Een meerwaarde bieden in vergelijking met de huidige 3 stelsystemen

Verwachtingen: flexibiliteit, eenvoud en grotere toegankelijkheid ten opzichte van de huidige systemen, namelijk:

- Stemmen op papier
- Elektronisch stemmen
- Stemmen per post

BN007 Moderniseren van het stemmen

Het systeem moet geheel of gedeeltelijk gebruik maken van moderne informatietechnologieën om:

- De huidige stelsystemen geheel of gedeeltelijk te dematerialiseren;
- Menselijke handelingen geheel of gedeeltelijk te automatiseren door geautomatiseerde processen;
- De snelheid te verhogen waarmee burgers kunnen stemmen, stemmen tellen en resultaten publiceren.

BN008 Beheersen van de kostprijs van de oplossing

De inrichtende macht moet zich bewust zijn van de jaarlijkse kosten voor het onderhouden en updaten van het systeem, om te garanderen dat het systeem altijd operationeel is vanuit functioneel en veiligheidsoogpunt. Bij deze kosten moet rekening worden gehouden met de "fulltime" interne middelen die nodig zijn tijdens niet-verkiezingsperioden.

8 Evaluatie van de risico's

Veiligheidsrisico's Impact- en waarschijnlijkheidsindicatoren volgens de volgende schaal:

- High: de impact of waarschijnlijkheid van het risico is hoog
- Medium: de impact of waarschijnlijkheid van het risico is middelgroot
- Low: de impact of waarschijnlijkheid van het risico is laag

RISK001	De oplossing staat bloot aan cyberaanvallen	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het hybride systeem is beschikbaar via het internet en staat daarom bloot aan cyberaanvallen.			
RSK002	De integriteit van de gegevens van de oplossing wordt bedreigd.	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het hybride systeem is beschikbaar via het internet en staat daarom bloot aan cyberaanvallen die de integriteit van de gegevens van de oplossing kunnen bedreigen. In het geval van de oplossing zijn er geen elektronische stembussen en dus geen stemgegevens, maar de impact op de betrouwbaarheid van deze methode zou zeer groot zijn.			
RSK003	De identiteit van de kiezer kan gestolen worden	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het hybride systeem is beschikbaar via het internet, op ongecontroleerde werkstations waar de authenticatie wordt uitgevoerd door een ongecontroleerde gebruiker.			
RSK004	De authenticiteit van de stem kan veranderd worden	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Aangezien de stem niet wordt gevalideerd door een stemopnemer, niet door de kiezer zelf wordt uitgebracht en alleen per post wordt verstuurd, kan de oprechtheid van de stem in twijfel worden getrokken/veranderd omdat het onmogelijk is om te garanderen dat de kiezer niet is beïnvloed. De organisatie van een massale stemming voor een bepaalde kandidaat of een bepaald voorstel kan niet worden uitgesloten.			
RSK005	De authenticiteit van de stem kan veranderd worden	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Omdat er per post gestemd wordt (voor mensen die niet op de dag zelf naar het stemlokaal gaan), kan de post zoekraken en de nauwkeurigheid van de stemming beïnvloeden.			
RSK006	Het stemgeheim kan in twijfel worden getrokken	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Mensen stemmen thuis op een onbeveiligde, onbetrouwbare computer, die geen garantie biedt dat een kwaadaardig programma de handelingen van de gebruiker en dus mogelijk ook de stemming niet registreert.			
RSK007	De architectuur van de oplossing kan veiligheidslekken vertonen.	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
De architectuur van de oplossing kan beveiligingslekken bevatten die bijgevolg misbruikt kunnen worden. De architectuur van de oplossing bevat verschillende componenten waarvan de beheerdersrechten beveiligingslekken kunnen openen of softwareversies die niet zijn bijgewerkt of verouderd zijn.			
RSK008	De ontwikkeling van de oplossing is gebrekkig	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)

De oplossing kan beveiligingsfouten in de code bevatten (injectie van kwaadaardige code, gebruik van verouderde bibliotheken, enz.).

Conclusie:

Technisch gezien bevat de hybride oplossing geen elektronische stembus waarin de stemmen worden opgeslagen. Stemmen zou alleen per post gaan, dus de nauwkeurigheid van de stemming zou beïnvloed worden door post die niet ontvangen wordt (een kleine maar reële kans, aangezien stemmen per post al bestaat).

We kunnen ervan uitgaan dat technische tekortkomingen met betrekking tot de architectuur, geprivilegieerde accounts en kwaadaardige code kunnen worden beperkt door controles op het niveau van de definitie van de architectuur, de ontwikkeling van de code, het beheer van de toegangen en de controle op wijzigingen die worden aangebracht in componenten (firewallregel, bijvoorbeeld).

Helaas is het met deze oplossing echter **vrijwel onmogelijk** om het volgende te garanderen:

- **De identiteit van de kiezer:** de authenticatie wordt op afstand uitgevoerd, zonder de mogelijkheid om de identiteit te valideren van de persoon die de transactie uitvoert.
- **De oprechtheid van de stem:** de stem wordt op afstand uitgebracht en genereert een stembiljet. Het gebeurt niet in een stemhokje en kan worden beïnvloed door een derde partij.
- **Het stemgeheim:** het stemgeheim kan niet worden gegarandeerd. Het is heel goed mogelijk om massale stemmingen te organiseren zonder dat dit ontdekt kan worden.

De risico's verbonden aan deze stemmethode hebben een grote impact op de hierboven beschreven pijlers. De huidige traditionele manier van stemmen, waarbij de kiezer fysiek aanwezig is in het stemhokje en een stembiljet of stemmachine gebruikt, wordt nu al beïnvloed door internetcampagnes en ondermijnt het vertrouwen van de kiezer in de uitkomst van de verkiezingen. Niet weten wie er echt gestemd heeft, of de stem de ware wens van de persoon was en de mogelijkheid van een geleide massale stemming, zonder garantie voor de anonimiteit van de stem, zou dit groeiende wantrouwen alleen maar accentueren.

9 Vereisten

Bedrijfs-, functionele, niet-functionele, technische en beveiligingsvereisten. De oplossing zal absoluut aan de prioritaire vereisten moeten voldoen.

- **MUST** = De oplossing kan niet worden geïmplementeerd tenzij aan de eis wordt voldaan. MVP (Minimum Viable Product).
- **SHOULD** = De oplossing kan in een eerste versie worden geïmplementeerd zonder dat aan de eis wordt voldaan, op voorwaarde dat de eis in een toekomstige versie wordt opgenomen.
- **COULD** = Dit is een "Nice to have", het niet voldoen aan deze eis is geen blokkerend punt voor de aanvaarding.

9.1 Bedrijfsvereisten

Business Requirements [BR].

De bedrijfsvereisten zijn wat het systeem moet doen om aan de geuite bedrijfsbehoeften te voldoen. De bedrijfsvereisten beschrijven de karakteristieken van een systeem vanuit het oogpunt van de eindgebruiker van dat systeem. Het systeem is een middel om bedrijfsdoelstellingen te leveren, te vervullen of eraan te voldoen.

BR001	Globaal en uniek systeem	Prio (Must / Should / Could)
Het hybride systeem moet kunnen worden gebruikt voor alle verkiezingen die door de federale overheid worden georganiseerd (federale, regionale en Europese verkiezingen) en voor alle soorten kiezers (stemmen in België en stemmen van Belgen in het buitenland). Het hybride systeem moet ook gebruikt worden voor vervroegde verkiezingen, d.w.z. het moet bruikbaar zijn tijdens de hele periode van vervroegd stemmen.		
BR002	Naleving van de Belgische grondwettelijke stemprincipes	Prio (Must / Should / Could)
De fundamentele elementen van het Belgische kiesstelsel zijn vastgelegd in de Grondwet:		
1. De verkiezingen vinden plaats volgens het algemeen stemrecht		
Het algemeen stemrecht geeft alle burgers de kans om hun mening te uiten zonder beperkingen wat betreft rijkdom of erfelijkheid.		
2. Het principe van evenredige vertegenwoordiging wordt toegepast		
Een evenredig systeem is een kiesstelsel dat aan elke lijst een aantal verkozenen toekent dat evenredig is met het aantal stemmen dat deze lijst heeft gekregen.		
3. Elke kiezer heeft één stem (behalve in het geval van een gevolmachtigde)		
De verschillende verkiezingen hebben drie voorwaarden gemeen om te mogen stemmen:		
<ul style="list-style-type: none">- Minstens 18 jaar oud zijn. Behalve voor de Europese verkiezingen (vanaf 2024), waar 16- en 17-jarigen kunnen kiezen om te stemmen als ze dat willen.- Ingeschreven zijn in het bevolkingsregister van een Belgische gemeente op de dag dat de kiezerslijst wordt afgesloten (de inschrijving in het vreemdelingenregister van de gemeente geldt voor de Europese en gemeenteraadsverkiezingen).- Niet het voorwerp uitmaken van een gerechtelijke beslissing die het kiesrecht schorst.		

4. De stemming is geheim

Het is onmogelijk om te zeggen wie wat gestemd heeft (a contrario wordt de stemming geannuleerd), behalve met de hulp van stembureauleden (die beëdigd zijn) of per volmacht:

- Bij een traditionele stemming (op papier) mogen de stembiljetten niet meteen in de stembus worden gedaan. Kiezers moeten het stemhokje binnengaan omdat niemand mag weten hoe ze hebben gestemd. Als een kiezer weigert het stemhokje binnen te gaan, wordt hij geregistreerd als een afwezige kiezer.
- Bij elektronisch stemmen moet de kiezer zijn elektronische kaart in de stemcomputer inbrengen en zijn stem uitbrengen of een blanco stem uitbrengen en het door de computer afgedrukte stembiljet innemen. Als de kiezer het stemhokje verlaat zonder stembiljet, wordt de kiezer als afwezig geregistreerd.

5. De stemming is verplicht

Elke Belgische burger die aan de bovenstaande voorwaarden voldoet, is verplicht om te stemmen. Het niet uitoefenen van dit recht stelt hem bloot aan sancties. Als het voor een burger onmogelijk is om persoonlijk te gaan stemmen, kan hij zijn stem uitbrengen via een vertrouwenspersoon.

- Belgen in België (vanaf 18 jaar op de dag van de verkiezingen) hoeven vooraf geen bijzondere stappen te ondernemen. Als ze voldoen aan de vier hierboven vermelde voorwaarden om te stemmen, krijgen ze automatisch een oproeping.
- Europese buitenlanders die in België aan de Europese verkiezingen deelnemen, moeten zich laten registreren.
- Belgen tussen 16 en 18 jaar (op de dag van de verkiezingen) die in België aan de Europese verkiezingen deelnemen, moeten zich laten registreren.
- Belgen in het buitenland zijn alleen verplicht om te stemmen als ze zich vooraf hebben geregistreerd. Als ze niet geregistreerd zijn, is stemmen niet verplicht.

6. Er wordt gestemd in de gemeente

De stemming vindt plaats in de gemeente waar de kiezer woont.

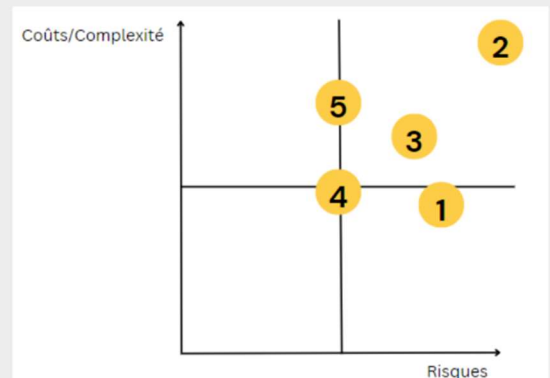
Tijdens een workshop met IBZ op 15 februari 2023 rangschikten de deelnemers de verschillende fundamentele criteria voor het uitvoeren van de studie in volgorde van belangrijkheid. Deze criteria werden gezamenlijk gerangschikt in de volgende volgorde:

- 1) Nauwkeurigheid van de resultaten
- 2) Veiligheid
- 3) Geheim van de stemming
- 4) Validatie van de verkiezing
- 5) Transparantie

Vervolgens plaatsten we ze op een matrix in termen van de kosten/complexiteit van implementatie en de risico's van niet-implementatie.

Critères fondamentaux

- 1 EXACTITUDE DES RÉSULTATS
- 2 SÉCURITÉ
- 3 SECRET DU VOTE
- 4 VALIDATION DE L'ÉLECTION
- 5 TRANSPARENCE



Critères fondamentaux	Fundamentele criteria
EXACTITUDE DES RÉSULTATS	NAUWKEURIGHEID VAN DE RESULTATEN
SÉCURITÉ	VEILIGHEID
SECRET DU VOTE	GEHEIM VAN DE STEMMING
VALIDATION DE L'ÉLECTION	VALIDATIE VAN DE VERKIEZING
TRANSPARENCE	TRANSPARANTIE
Coûts/Complexité	Kosten/Complexiteit
Risques	Risico's

BR003 Evolutive architectuur

Prio (Must / Should / Could)

De oplossing moet onafhankelijke, onderling verbonden componenten bevatten die kunnen worden hergebruikt in een upgrade van de oplossing of in de versies "stemmen in België" en "stemmen van Belgen in het buitenland". Dit principe garandeert een zekere rationaliteit en efficiëntie in kostenbeheersing.

BR004 Beheer van wijzigingen

Prio (Must / Should / Could)

Dit nieuwe systeem moet uitgelegd en begrepen worden door de vertegenwoordigers van de inrichtende macht en door de leden van de onthaal-/tellingbureaus die het systeem zullen gebruiken.

BR005 Beheer van de faciliteitengemeenten Prio (Must / Should / Could)

Dit zijn gemeenten die, in de zin van de toepassing van de wetten op het gebruik van talen in administratieve aangelegenheden, genieten van een systeem van taalkundige faciliteiten ten voordele van hun inwoners. De wet van 8 november 1962 voorzag in vijf categorieën gemeenten die konden afwijken van de regel van territoriale eentaligheid (met een minimum van 30% minderheden) zonder de status van tweetalige gemeente te verwerven (behalve in Brussel).

"Faciliteitengemeenten" worden gekenmerkt door eentalige interne diensten (de administratie werkt in één taal) en externe tweetaligheid (de administratie gebruikt twee talen in haar contacten met het publiek).

BR006 Procedure voor coördinatie met belanghebbenden

Prio (Must / Should / Could)

Opstellen van een coördinatieprocedure met de accreditatieorganisatie, het cybercriminaliteits- en defensiecentrum, het college van deskundigen (vertegenwoordigers van de verschillende vergaderingen) en de betrokken toezichthoudende organen.

9.2 Functionele vereisten

Functional Requirements [FR].

De functionele vereisten (FR- Functional Requirements) zijn een verklaring over hoe een systeem zich moet gedragen. Ze definiëren wat het systeem moet doen om aan de bedrijfsbehoeften te voldoen. De functionele vereisten kunnen worden gezien als kenmerken die de gebruiker detecteert.

FR001 Invoeren van gegevenslijsten (Data File Transfer) Prio (Must / Should / Could)

- Lijst van Belgische kiezers die in België wonen, invoer van de kiezerslijst uitgegeven door de gemeenten.
- Lijst van Belgische kiezers die in het buitenland wonen, invoer van de kiezerslijst uitgegeven door de beroepsconsulaire posten/diplomatieke posten.
- Lijst van politieke partijen, invoer van de lijst van partijen uitgegeven door de algemene stembeheermodule.
- Lijst van kandidaten, invoer van de lijst van kandidaten uitgegeven door de algemene stembeheermodule.

FR003 Unieke authenticatie

Prio (Must / Should / Could)

De kiezer maakt verbinding met de website en authenticceert zich.

Kiezers authenticeren zich slechts eenmaal per sessie om toegang te krijgen tot alle functies:

- Afdruk van de stembiljetten
- Afdruk van de etiketten voor verzending
- Generatie van de 'K'-verificatiecode

FR004 "Gebruiksvriendelijke" interface Prio (Must / Should / Could)

Gebruiksvriendelijke, ergonomische en intuïtieve interface voor kiezers die toegang willen tot het hybride systeem.

Het systeem moet zoveel mogelijk toegankelijk zijn voor alle gebruikers, inclusief ouderen, kleurenblinden, slechtzienden en mensen met een handicap.

Het belangrijkste doel van een gebruiksvriendelijke interface is om een zo bevredigend mogelijke gebruikerservaring te bieden: grafische interface, gemakkelijk herkenbare invoerzones, grootte van de invoerzones, grootte van de tekens, natuurlijke gebruikerstaal, enz.

FR005 Zelfbediening

Prio (Must / Should / Could)

Na je ingelogd en geïdentificeerd te hebben,

- Met het systeem kunnen kiezers hun stembiljet(ten) en etiketten voor dubbele omslagen afdrukken.
- Na gestemd te hebben en eenmaal de stemopnemingsverrichingen beëindigd zijn, biedt het systeem de kiezer de mogelijkheid om zijn 'K'-verificatiecode te coderen en toegang te krijgen tot de status van de codering van zijn stem(men) in het systeem door de bijzitters.

FR006 Genereren van de 'K'-verificatiecode

Prio (Must / Should / Could)

Nadat de kiezer is ingelogd en zich heeft geïdentificeerd, wordt hem gevraagd de 'K'-verificatiecode te genereren, zodat hij kan controleren of zijn stem in aanmerking is genomen, zodra deze is ontvangen en geteld.

FR007 Unieke authenticatie Prio (Must / Should / Could)

De unieke authenticatie is een methode die een gebruiker toegang geeft tot verschillende systeemfuncties (afdrukken van stembiljetten, afdrukken van etiketten, opvragen van de 'K'-verificatiecode, controleren of de stem in aanmerking is genomen) door middel van eenmalige aanmelding.

FR008 Beheren van het meervoudig stemmen Prio (Must / Should / Could)

- Voorkomen van het uitbrengen van meerdere stemmen tussen in persoon stemmen en stemmen via het hybride systeem.
Een in persoon uitgebrachte stem heeft voorrang op alle andere stemmen. Als de kiezer meerdere stelsystemen gebruikt, is de in persoon uitgebrachte stem de enige die in aanmerking wordt genomen, ongeacht of de kiezer stemt met een geldig, verdacht of blanco/ongeldig stembiljet.
- Voorkomen van het uitbrengen van meerdere stemmen in het hybride systeem zelf.
Op basis van de 'K'-verificatiecode geeft het systeem aan of een stem al ingevoerd werd. Als er meer dan één stem werd ingevoerd, wordt alleen met de eerste stem rekening gehouden.
- Vanuit het oogpunt van organisatorische complexiteit is het niet de bedoeling dat de hybride, kiosk- en volledig online systemen tegelijkertijd operationeel zullen zijn voor één gemeente.
- Informeren van de kiezer: koppelen van een bericht aan de 'K'-verificatiecode.

FR009 Raadplegen en opzoeken Prio (Must / Should / Could)

Kiezers kunnen naar wens inloggen op het systeem nadat ze zich hebben geauthenticeerd. Dankzij de 'K'-verificatiecode:

- Ze kunnen controleren of hun stem correct is ingevoerd in het systeem. Hiertoe stuurt het systeem een bevestigingsbericht.
- Het systeem geeft aan of er meer dan één stem is ontvangen en wat het resultaat is van de verwerking van de meervoudige stem.

FR010 Data Anonymisation, Pseudonymisation Prio (Must / Should / Could)

Anonimisering en pseudonimisering van gegevens hebben tot doel private, gevoelige of vertrouwelijke informatie uit de ruwe gegevens te maskeren. Het resultaat zijn gegevens die met geen enkel individu in verband kunnen worden gebracht.

Anonimisering en pseudonimisering van gegevens is een manier om een valse maar realistische versie van organisatiegegevens te creëren. Het doel is om gevoelige gegevens te beschermen en tegelijkertijd een functioneel alternatief te bieden wanneer echte gegevens niet nodig zijn. Bij anonimisering kan de broninformatie niet worden geregenereerd, wat wel kan bij pseudonimisering. Er wordt gekozen voor anonimisering, pseudonimisering wordt afgewezen.

Anonimisering wordt toegepast voor:

- Het creëren van testsets om het hybride systeem te testen
- Het maskeren van de gegevens in het hybride systeem

FR011 Toegangsbeheer Prio (Must / Should / Could)

Het betreft hier de planning, de ontwikkeling en de uitvoering van beveiligingsrichtlijnen, -processen en -procedures om een gepaste authenticatie, autorisatie, toegang en audit mogelijk te maken.

- De juiste toegangen activeren en ongepaste toegangen voorkomen.
- Alle relevante regels en beleidsrichtlijnen op het gebied van privacy, bescherming en vertrouwelijkheid begrijpen en naleven.
- Ervoor zorgen dat de privacy- en vertrouwelijkheidsbehoeften van alle belanghebbenden worden toegepast en gecontroleerd.

FR012 Publicatie van de resultaten Prio (Must / Should / Could)

De stembiljetten voor het hybride systeem (vooraf stemmen) worden gereserveerd en geteld na het afsluiten van het stemmen in persoon. Verder is het verboden om gedeeltelijke vervroegde resultaten vast te stellen.

9.3 Niet-functionele vereisten

Non Functional Requirements [NFR].

Een "niet-functionele vereiste" houdt een beperking in op de oplossing. Het gaat meestal om hoge prestaties, volume, beschikbaarheid, schaalbaarheid, enz.

NFR001	Beleid inzake het bewaren van gegevens	Prio (Must / Should / Could)
<p>De databewaringstermijn moet worden gedefinieerd, in overeenstemming met het dataretentiebeleid dat wordt toegepast op de verschillende stelsystemen.</p> <p>De ontvangen stembiljetten worden bewaard totdat de stemmen zijn gevalideerd. Daarna worden ze vernietigd (in overeenstemming met de procedures die in het kader van de stemming op papier worden toegepast).</p> <p>Voor de ontwikkelings- en testperiode kan een specifiek beleid worden toegepast.</p> <p>Op basis van deze periode zal een geautomatiseerd proces verouderde gegevens uit de opslag van het hybride systeem verwijderen.</p>		
NFR002	Prestatie	Prio (Must / Should / Could)
<p>Elke transactie heeft een maximale reactietijd van 2 seconden, zodat de gebruiker onmiddellijk feedback krijgt.</p> <p>Generatie in pseudo-realtime van de 'K'-verificatiecode bij het aanvragen van het afdrukken van stembiljet(ten) en etiketten. Een latentie van minder dan 1 seconde wordt geaccepteerd.</p>		
NFR003	Service Level Agreement	Prio (Must / Should / Could)
<p>De SLA moet worden gedefinieerd voor elk onderdeel van het systeem (backend, frontend, opslag, middleware, enz.).</p> <p>De Service Level Agreement (SLA) is een gedocumenteerde overeenkomst die de kwaliteit van de dienstverlening definieert, een voorgeschreven prestatie tussen de systeemontwikkelaar en de inrichtende macht.</p> <p>Het gaat om clausules op basis van een contract waarin de precieze doelstellingen worden gedefinieerd die worden verwacht en het serviceniveau dat wordt gewenst door de inrichtende macht, en waarin de verantwoordelijkheden worden vastgelegd. Dit dient als basis voor het monitoren van het systeem in productie.</p>		
NFR004	RTO – Recovery Time Objective	Prio (Must / Should / Could)
<p>De "Recovery Time Objective" (RTO) of hersteltijd-doelstelling is de streefduur en het serviceniveau waarbinnen een bedrijfsproces moet worden hersteld na een onderbreking om een verstoring van de bedrijfscontinuïteit te voorkomen.</p> <p>De verwachte RTO is bijna 0 seconden op de onderdelen backend, opslag en frontend, voor de periode van vervroegd stemmen, d.w.z. (D-7) totdat de verkiezing is gevalideerd.</p> <ul style="list-style-type: none">- SLA-niveau = 99.96%- Downtime□/onbeschikbaarheid per dag = 35 seconden- Downtime□/onbeschikbaarheid per week = 4 minuten 1,9 seconden- Downtime□/onbeschikbaarheid per maand = 17 minuten 23 seconden- Downtime□/onbeschikbaarheid per kwartaal = 52 minuten 9,8 seconden- Downtime□/onbeschikbaarheid per jaar = 3 uur 28 minuten 39 seconden		

De verwachte RTO kan langer zijn buiten de periode van vervroegd stemmen, d.w.z. (D-24) totdat de verkiezing is gevalideerd.

- SLA-niveau = 99.900%
- Downtime□/onbeschikbaarheid per dag = 1 minuut 26 seconden
- Downtime□/onbeschikbaarheid per week = 10 minuten 5 seconden
- Downtime□/onbeschikbaarheid per maand = 43 minuten 28 seconden
- Downtime□/onbeschikbaarheid per kwartaal = 2 uur 10 minuten 24 seconden
- Downtime□/onbeschikbaarheid per jaar = 8 uur 41 minuten 38 seconden

NFR005 RPO – Recovery Point Objective

Prio (Must / Should / Could)

Een "Recovery Point Objective" (RPO) of herstelpuntdoelstelling is het maximaal aanvaardbare interval waarin transactionele gegevens van een IT-service verloren gaan. De RPO wordt bepaald door de tijd tussen gegevensback-ups en de hoeveelheid gegevens die verloren zou kunnen gaan tussen back-ups te onderzoeken. De verwachte RPO is 0 seconden.

NFR006 Belasting in een multi-user context Prio (Must / Should / Could)

De oplossing moet bestand zijn tegen een aanzienlijke belasting. Kiezers zullen niet allemaal op hetzelfde moment inloggen om stembiljetten en etiketten af te drukken en de 'K'-verificatiecode te genereren, maar het aantal is aanzienlijk (basis = jaar 2019: stemmen in België + stemmen van Belgen in het buitenland = 8.167.709, en aantal stembiljetten = 7.218.036).

NFR007 Tests Prio (Must / Should / Could)

De types van tests, protocollen en resultaten worden gepubliceerd voordat het systeem in productie gaat:

- Schaalbaarheidstest (basis = jaar 2019: stemmen in België + stemmen van Belgen in het buitenland = 8.167.709, en aantal stembiljetten = 7.218.036)
- Systeem inbraaktest
- Beveiligingstest gegevenstoegang, cfr OWASP-kwetsbaarheid, statisch en dynamisch
- DRtest – Disaster Recovery
- Unittests (minimum 80%)
- UAT
- Geautomatiseerde functionele tests
- Handmatige functionele tests
- Penetratietests (interne en externe vijandige agenten)
- Veiligheidstests
- Integratietests
- Non-regressietests
- SCA- Software Composition Analysis

De testprotocollen worden vooraf ter validatie naar de accreditatieorganisatie gestuurd. De resultaten worden naar de accreditatieorganisatie gestuurd als input voor hun procedures voor de validatie van het hybride systeem.

NFR008 Hoge beschikbaarheid Prio (Must / Should / Could)

24 uur per dag, 7 dagen per week, tijdens de periode van vervroegd stemmen, d.w.z. (D-24) totdat de verkiezing is gevalideerd.

NFR009 IT-ondersteuning Prio (Must / Should / Could)

De IT-leverancier houdt toezicht op en biedt IT-ondersteuning voor het systeem aan de inrichtende macht.

De IT-leverancier biedt geen eerstelijns-ondersteuning aan burgers die willen stemmen (zie OUT013).

De IT-leverancier produceert volledige documentatie, d.w.z. over de functionele en technische aspecten, onafhankelijk van de serviceovereenkomst.

De accreditatieorganisatie is betrokken bij het verkiezingsproces.

Het cybercriminaliteits- en defensiecentrum is betrokken bij het verkiezingsproces.

NFR010 Betrouwbaarheid - Fault Tolerant Process

Prio (Must / Should / Could)

De processen voor gegevensinvoer, -generatie, -transformatie en -restitutie moeten storingstolerant zijn.

Bij een storing moeten de processen correct herstarten waar ze gebleven waren.

Er moet minimaal automatisch een waarschuwing worden verstuurd en processen die zijn mislukt moeten handmatig opnieuw kunnen worden gestart.

NFR011 Naleving van het privacybeleid voor gegevens - AVG

Prio (Must / Should / Could)

Principes die moeten worden nageleefd in de context van de Belgische grondbeginselen.

Persoonsgegevens mogen alleen worden gebruikt met toestemming van de betrokkene voor het bekende doel, door de voorwaarden te accepteren.

Wanneer een betrokkene zich terugtrekt:

- Er mogen geen persoonlijke gegevens meer worden verzameld.
- Eerder verzamelde persoonsgegevens mogen niet worden gebruikt in de verwerking.

Wanneer een betrokkene zich aanmeldt:

- Persoonsgegevens worden verzameld en gebruikt door de verwerking met betrekking tot het doel waarvoor de betrokkene toestemming heeft gegeven door in te stemmen met de voorwaarden en alle beginselen van de AVG te volgen, bijv. "Minimalisatiebeginsel".

Wanneer een betrokkene zijn/haar recht om te worden gewist (recht om te worden vergeten - art. 17 van de AVG) uitoefent, moeten al zijn/haar persoonsgegevens worden gewist uit alle opslagmedia, maar ook uit toepassingen en rapporten waarin ze kunnen worden geïdentificeerd. In bepaalde gevallen kan pseudo-anonimisering (Art. 32°, Art. 25°, andere van de AVG) of anonimisering worden toegepast.

In de specifieke context van de Belgische verkiezingen zijn de beginselen en de verschillende kiesreglementen die in het kader van de Belgische grondwettelijke beginselen moeten worden nageleefd:

- Alle gegevens, inclusief persoonsgegevens, worden onmiddellijk na de validering van de verkiezingen gewist.
- Het recht om te worden vergeten kan niet afwijken van deze beginselen en verkiezingsregels.

Dit reglement is dus in overeenstemming met de AVG.

9.4 Technische vereisten

Technical Requirements [TR].

Een "Technische Vereiste" houdt een beperking in op het technische ontwerp van de applicatiecomponenten van de oplossing.

TR001	Web GUI – Graphical User Interface	Prio (Must / Should / Could)
<p>Ergonomische en intuïtieve grafische interface zodat kiezers toegang hebben tot het hybride systeem.</p> <p>Naleving van de <i>look-and-feel</i> die door IBZ is voorgesteld en/of door de andere verkiezingsmodules en de softwarebibliotheek van manipuleerbare objecten (widgets) is vastgesteld. De <i>look-and-feel</i> is een verzameling regels voor de visuele presentatie en het gedrag van grafische interfaces. De presentatieregels hebben met name betrekking op het gebruik van kleuren, typografie, de presentatie en betekenis van logo's en pictogrammen, de presentatie van vensters (locatie, vorm en gedrag van widgets) en cursorvormen. Gedragsregels bepalen hoe visuele elementen reageren op gebruikersacties (muisbewegingen, indrukken van muis- en toetsenbordknoppen).</p> <p>De toepassing van deze regels is bedoeld om het leren te vergemakkelijken en de gebruikerstevredenheid te verbeteren.</p>		
TR002	Gegevensinvoer	Prio (Must / Should / Could)
<p>Invoer van gegevensbestanden voor de lijst van kiezers, partijen en kandidaten. Het formaat van de gegevensbestanden moet overeenkomen met dat van de bestanden die momenteel door de andere verkiezingsmodules worden verwerkt. EML-formaat (Election Markup Language), definitie op Europees niveau van de XML-bestanden (Extensible Markup Language) die voor verkiezingen worden gebruikt.</p>		
TR003	Formaat van de stembiljetten	Prio (Must / Should / Could)
<p>De opmaak van het formaat van het stembiljet is A4. Alleen RECTO-afdrukken. De informatie op het A4-document moet coherent en leesbaar zijn voor de kiezers: verdeel de lijsten niet over twee vellen.</p>		
TR004	IAM – Identity & Access Management	Prio (Must / Should / Could)
<p>Sterk authenticatiesysteem: CSAM (eID en itsme). CSAM is een identiteits- en toegangsbeheersysteem voor e-government en binnen het Europese eIDAS-kader. Het systeem werd opgezet door de Belgische federale overheid. Het systeem maakt identificatie, authenticatie, autorisatie en beheer van mandaten mogelijk. CSAM is een samenwerking tussen de RSZ, het Directoraat-generaal Digitale Transformatie, de FOD Financiën, de Kruispuntbank, de FOD Economie, KMO, Middenstand en Energie en de FOD Binnenlandse Zaken. De eerste overeenkomsten werden ondertekend in 2011, maar het duurde tot 2013 vooraleer het systeem actief werd. Kiezers kunnen zich via CSAM aanmelden met een beveiligingscode, via een authenticatietoepassing, eID of via de itsme-toepassing. Inloggen via een token, een beveiligingscode via e-mail of een ander alternatief systeem is ook mogelijk, op voorwaarde dat het beveiligingsniveau vergelijkbaar of hoger is.</p>		

Access Repository. Autorisatiesysteem gebaseerd op:

- De kieslijsten ontvangen van de gemeenten voor Belgische kiezers die in België stemmen, van beroepsconsulaire/diplomatieke posten
- De samenstelling van de bureaus:
 - o De lijst van de voorzitters van de ontvangst-/stemopnemingsbureaus (hoofd- en plaatsvervangers)
 - o De lijst van de bijzitters van de ontvangst-/stemopnemingsbureaus (hoofd- en plaatsvervangers)
 - o De lijst van de getuigen van de ontvangst-/stemopnemingsbureaus
 - o De lijst van de leden van de griffie van het Gerecht van eerste aanleg
 - o De lijst van de leden van de griffie van het Vredegerecht
- De lijst van de andere tussenkomenende partijen

Toegangscontrole: er moet een gedetailleerde beschrijving zijn van alle rollen (groepen, privileges, autorisaties) die in het systeem worden gebruikt en de exacte toegangsrechten (functionaliteiten en gegevens) voor elke rol. Een toegangscontrolematrix heeft de voorkeur voor deze regels.

TR005 Integriteit van het stemsysteem Prio (Must / Should / Could)

Alleen de systeemontwerpers, de accreditatieorganisatie, het college van deskundigen en de inrichtende macht hebben toegang tot de niet-gecompileerde en gecompileerde code.

Op verzoek van de verschillende belanghebbenden (die de bevoegdheid hebben om dit verzoek te doen) mag de code worden gepubliceerd, op voorwaarde dat de beveiligingscode wordt verwijderd.

TR006 Beheer van de meertaligheid Prio (Must / Should / Could)

Frans, Nederlands en Duits.

TR007 'On-the-fly' generatieproces voor de 'K'-verificatiecode Prio (Must / Should / Could)

Het proces voor het genereren van de 'K'-verificatiecode begint wanneer de kiezer vraagt om de stembiljetten en etiketten te printen.

TR008 Audit Trail Prio (Must / Should / Could)

Het is belangrijk om de geladen gegevens te kunnen traceren. Een 'Audit Trail'-functie archiveert de historiek van de stromen. Tijdens de uitvoering wordt relevante informatie met betrekking tot de toewijzing van resources en de status van uitgevoerde werkitens vastgelegd in Audit Trails.

TR009 De 'K'-verificatiecode kan met de hand worden gecodeerd Prio (Must / Should / Could)

De 'K'-verificatiecode kan met de hand worden ingevoerd op een toetsenbord. Geen QR-code of streepjescode.

TR010 Technische sleutel voor 'K'-verificatiecode Prio (Must / Should / Could)

Dit zorgt ervoor dat het onmogelijk is om de kiezer die het stembiljet heeft uitgebracht te identificeren. Het kan gebaseerd zijn op kiezersgegevens, op voorwaarde dat deze gegevens anoniem worden gemaakt (onmogelijk om terug te gaan) aan het begin van het genereren van de 'K'-verificatiecode.

TR011	Verwerken van grote datavolumes	Prio (Must / Should / Could)
	<p>Het datavolume is niet gekoppeld aan de hoeveelheid informatie per kiezer, maar aan het aantal kiezers.</p> <p>Er zijn Processing Engines van de juiste grootte nodig om parallelle verwerking mogelijk te maken.</p>	
TR012	Monitoring, Logging and Alerting	Prio (Must / Should / Could)
	<p>Het systeem moet worden gemonitord en gebeurtenissen moeten worden gelogd (operationele en beveiligingslogs) in de verschillende onderdelen, van de invoer van gegevens tot de weergave en het gebruik van gegevens in rapporten en dashboards.</p> <p>Er moet ook een waarschuwingsmechanisme zijn in geval van storingen, gebaseerd op de vooraf gedefinieerde SLA.</p>	
TR013	CI/CD – Release Management	Prio (Must / Should / Could)
	<p>Het concept van CI/CD is een combinatie van de twee praktijken van continue integratie (CI) en continue levering of continue uitrol (CD).</p> <p>Hoewel het vaak samen wordt gezien, impliceert het ene niet noodzakelijk het andere.</p> <p>CI houdt in dat bij elke wijziging van de code wordt gecontroleerd of er geen regressie is. Het doel is om integratieproblemen zo vroeg mogelijk in het ontwikkelproces te identificeren. Deze praktijk is wenselijk.</p> <p>CD houdt in dat het systeem in zeer korte cycli wordt geproduceerd. Het doel is om heel snel te bouwen, te testen en uit te rollen. Deze praktijk is niet wenselijk in de context van:</p> <ul style="list-style-type: none"> - een systeem dat zo cruciaal is als het stelsysteem - een 'Release Management (Fixed Release)'-logica - een 'Code Review/Audit'-logica - de accreditatielogica. <p>CI is een gewenste praktijk om automatisering tijdens de ontwikkelperiode mogelijk te maken.</p> <p>Om een beheerst 'Release Management' te bereiken, moet een CI/CD-proces worden gedefinieerd en ondersteund door een set tools.</p>	
TR014	Scheduler	Prio (Must / Should / Could)
	<p>De geautomatiseerde processen moeten geprogrammeerd en gepland worden met behulp van een planner. Deze planner moet het ook mogelijk maken om waarschuwingsmechanismen te definiëren indien nodig.</p> <p>Bijvoorbeeld: het nemen van back-ups, mogelijkheid om stemmen alleen in te voeren als het stemlokaal gesloten is (om dubbeltelling te voorkomen).</p>	
TR015	Disaster Recovery Plan (DRP)	Prio (Must / Should / Could)
	<p>In het geval van een ramp moet het systeem operationeel zijn zonder vertraging (0 seconde) in overeenstemming met de SLA, RTO's en RPO's.</p> <p>Er moet een gedocumenteerd DRP worden opgesteld.</p>	
TR016	Back-up en archivering van gegevens	Prio (Must / Should / Could)
	<p>Er moet een gegevensback-up worden geïmplementeerd in overeenstemming met de gedefinieerde criteria (zie RTO's en RPO's).</p>	
TR017	Back-up van de code en de configuratieparameters	Prio (Must / Should / Could)
	<p>Een back-up van de ontwikkelingscodes en systeemconfiguratieparameters moet worden geïmplementeerd op basis van de SLA.</p>	

TR018	Code Versioning	Prio (Must / Should / Could)
Er moet een krachtige tool voor het beheer van de codeversies worden geïmplementeerd om: <ul style="list-style-type: none">- De verschillende versies en patches van de code te identificeren.- Een geschiedenis bij te houden van de verschillende versies en patches. Dit systeem is een aanvulling op de tool die certificeert dat de gecompileerde code die in productie wordt genomen (gecertificeerd en goedgekeurd) identiek is aan de code die werd gegenereerd, voor dezelfde versie. Deze tool garandeert ook dat de broncodecompilatieprocessen tot de verwachte gecompileerde resultaten leiden.		
TR019	Gegevensopslag	Prio (Must / Should / Could)
Er wordt een algemeen relationeel databasebeheersysteem gebruikt.		
TR020	Broncode	Prio (Must / Should / Could)
De software heeft een goed gestructureerde broncode en is opgedeeld in modules, zonder functionele overlap. Elke module biedt een specifieke set functionaliteiten aan. Elke functionaliteit wordt gepresenteerd door slechts één module. Elke module bevat de nodige uitleg over de werking ervan.		
TR021	DTAP-omgevingen	Prio (Must / Should / Could)
Er zijn strikt gescheiden omgevingen voor ontwikkeling (D), tests (T), aanvaarding (A), opleiding en productie (P) voorzien.		
TR022	Gegevensversleuteling	Prio (Must / Should / Could)
De gegevensversleuteling moet het type gegevens specificeren dat geanonimiseerd moet worden, de methode die gebruikt wordt en de tool die gebruikt wordt. Deze software moet recente en publiekelijk geteste algoritmen zonder bekende kwetsbaarheden gebruiken.		
TR023	Accreditatie	Prio (Must / Should / Could)
De accreditatieorganisatie moet de broncode, configuratieparameters en infrastructuur (App SRV en Storage) valideren. De accreditatieorganisatie moet het gelijkvormigheidsattest verstrekken.		
TR024	Versleuteling van de overgedragen gegevens	Prio (Must / Should / Could)
<ul style="list-style-type: none">- De gegevens die tussen de verschillende modules overgedragen worden, moeten versleuteld zijn.- De opgeslagen gegevens moeten versleuteld zijn.		

9.5 Beveiligingsvereisten

Security Requirements [SEC].

Een "Beveiligingsvereiste" houdt een beperking in op het ontwerp van de oplossing die garandeert dat wordt voldaan aan beveiligingskenmerken zoals vertrouwelijkheid, integriteit en beschikbaarheid.

SEC001	Implementeren van een technische en organisatorische oplossing van hoge kwaliteit die geen grote kwetsbaarheden vertoont (kwetsbaarheden die door de uitgever zijn gepubliceerd en/of door derden openbaar zijn gemaakt).	Prio (Must / Should / Could)
	<ul style="list-style-type: none">- Gebruikmaken van de laatste ondersteunde en bijgewerkte versies van de besturingssystemen, webserver, encryptieoplossingen en databases die in de oplossing worden gebruikt.- Zich ervan vergewissen dat de nieuwste beveiligingsupdates worden toegepast.- Controleren of de veiligheidslekken in componenten van derden ook zijn gedekt.- Gebruikmaken van openbare encryptieprotocollen en algoritmen die als "sterk" worden beschouwd.-	
SEC002	Definiëren van de stem van een kiezer als een atomaire verrichting die bestaat uit de selectie, de validatie en de afgifte van een ontvangstbewijs	Prio (Must / Should / Could)
	Zodra de kiezer zijn of haar stemkeuze definitief heeft gevalideerd, moeten alle bovenstaande verrichtingen zonder onderbreking worden uitgevoerd totdat de laatste verrichting is voltooid, d.w.z. tot aan de afgifte van een ontvangstbewijs. Het mislukken van één actie resulteert in het mislukken van de hele keten en omgekeerd is het succes van de keten alleen mogelijk als elk van de unitaire acties correct wordt uitgevoerd.	
SEC003	Authenticeren van de kiezers door ervoor te zorgen dat de belangrijkste risico's in verband met identiteitsdiefstal aanzienlijk worden verminderd	Prio (Must / Should / Could)
	Kiezers authenticeren zich met behulp van oplossingen voor multifactorauthenticatie. In geval van verlies of diefstal van hun authenticatiemiddel, stelt een procedure de kiezer in staat om te stemmen en maakt deze het verloren of gestolen authenticatiemiddel onbruikbaar.	
SEC004	Voorkomen dat het systeem wordt blootgesteld aan bedreigingen voor de cyberveiligheid	Prio (Must / Should / Could)
	De architectuur moet de nodige verdedigingsmiddelen implementeren om cyberaanvallen (DDOS, Brute Force, enz.) te voorkomen. Voor WEB-toepassingen moet ook rekening worden gehouden met de belangrijkste kwetsbaarheden die door OWASP zijn gepubliceerd.	
SEC005	Gebruikmaken van een informatiesysteem dat de fysieke en logische beveiligingsmaatregelen implementeert die worden aanbevolen door uitgevers.	Prio (Must / Should / Could)
	Toepassen van de best practices in de documentatie van de uitgevers, in het bijzonder de uitgevers van stemoplossingen, alsook de uitgevers van webserver, applicatieserver en database-uitgevers.	
SEC006	Ervoor zorgen dat een interventieplan kan worden geactiveerd bij een veiligheidsincident	Prio (Must / Should / Could)

In het geval van een veiligheidsincident moet een interventieplan kunnen worden geïmplementeerd. Dit plan moet regelmatig worden herzien en volledig worden beheerst door alle betrokkenen.

SEC007 De integriteit van de registratie van de verrichtingen in het systeem waarborgen Prio (Must / Should / Could)

Elke verrichting die in het systeem wordt uitgevoerd, moet worden geregistreerd. De integriteit moet gegarandeerd zijn en de verrichting moet geraadpleegd kunnen worden zonder de inhoud ervan te wijzigen.

De logboeken van de verrichtingen moeten 3 maanden online en 1 jaar offline worden bewaard.

SEC008 Verzekeren van een beheer van de toegangen tot het systeem Prio (Must / Should / Could)

De toegang tot het systeem en de onderdelen ervan voor bevoorrechte accounts moet worden onderworpen aan:

- Toegangsbeheerproces met validatie door een goedgekeurde manager;
- Goede praktijken die het aantal van dergelijke accounts beperkt tot een maximum van 5 per component (serverbeheerders, databasebeheerders, enz.);
- Niet vrijgeven van wachtwoorden door het installeren van een PAM-component ("Privilege Access Management");
- 'Least Privilege'-principe voor alle geprivilegieerde accounts;
- Periodiek juridisch overzicht.

SEC009 Zorgen voor een opvolging van de kwetsbaarheden en patches Prio (Must / Should / Could)

Er moet voor een opvolging van de kwetsbaarheden gezorgd worden, alsook voor de toepassing van de patches indien beschikbaar. Zo niet, moeten er tegenmaatregelen worden voorgesteld om de kwetsbaarheden te verhelpen.

SEC010 Verzekeren van de opvolging van de versies van het systeem Prio (Must / Should / Could)

Elke update van het systeem, door ontwikkeling of door het updaten van een component, moet getraceerd worden samen met de gerelateerde wijzigingen. Om de oorsprong en integriteit van een nieuwe versie te garanderen, zal voor een hashing van de binaries worden gezorgd.

SEC011 Zich vergewissen van de dichtheid van de omgevingen Prio (Must / Should / Could)

De omgevingen die nodig zijn voor ontwikkeling, testen, acceptatie of productie moeten volledig dicht zijn, zonder mogelijke afwijkingen.

SEC012 Controleren van de integriteit van de ontwikkeling Prio (Must / Should / Could)

De aangeleverde code moet dagelijks gescand worden om de aanwezigheid van kwaadaardige code gedurende de gehele ontwikkelcyclus te voorkomen.

SEC013 Controleren van de integriteit van het systeem Prio (Must / Should / Could)

Het systeem zal regelmatig onderworpen worden aan veiligheidscontroles (Penetration Testing, Access Review, enz.).

SEC014 Definitie van een machtigingsmodel Prio (Must / Should / Could)

Er wordt een machtigingsmodel gedefinieerd waarin rollen en groepen worden gespecificeerd, evenals de bijbehorende rechten en toewijzings-/validatieprocessen.

SEC015 Logboek van de veiligheidsgebeurtenissen Prio (Must / Should / Could)

De veiligheidsgebeurtenissen worden gecodeerd, opgeslagen en gecategoriseerd. Ze worden zodanig opgeslagen dat hun integriteit gegarandeerd is (alleen lezen). Ze bevatten ten minste:

- Het tijdstip (uitgedrukt in UTC en gebaseerd op een betrouwbare bron);
- Het IP-adres en/of de systeemnaam van de betrokken systemen;
- De identiteit van de gebruiker en/of het systeem;
- Het beveiligingsniveau;
- De details van de gebeurtenis.

De veiligheidslogboeken moeten 3 maanden online en 1 jaar offline worden bewaard.

SEC016 Scheiding van de taken Prio (Must / Should / Could)

Het machtigingsmodel moet een functiescheidingsmatrix ("Segregation of Duties") specificeren. Het toegangsbeheer moet ervoor zorgen dat deze functiescheidingsregels worden geïmplementeerd.

SEC017 Toegang tot de productieomgevingen Prio (Must / Should / Could)

Toegang tot de productieomgeving moet worden beperkt en gevalideerd door de veiligheidsverantwoordelijke. Als zodanig heeft geen enkele ontwikkelaar toegang tot de productieomgeving.

SEC018 Aanstelling van de veiligheidsverantwoordelijken Prio (Must / Should / Could)

Er moeten veiligheidsverantwoordelijken worden aangesteld en kenbaar worden gemaakt in een organigram.

SEC019 Veiligheid van de hardware Prio (Must / Should / Could)

De apparatuur die door het systeem wordt gebruikt moet beveiligd zijn en zich in een ruimte bevinden met bewaakte en gecontroleerde fysieke toegang.

SEC020 Veiligheid van de ontwikkeling Prio (Must / Should / Could)

De ontwikkelingsrichtlijnen zijn gebaseerd op de best practices van OWASP, Application Security Verification Standard (ASVS) niveau 3 (maximumniveau).

SEC021 Veiligheid van de ontwikkelingscyclus Prio (Must / Should / Could)

De ontwikkelingscyclus (Secure Development Life Cycle) wordt uitgevoerd binnen een veilig en aantoonbaar raamwerk in overeenstemming met modellen zoals het Software Assurance Maturity Model (SAMM) van OWASP.

SEC022 Beperkte fysieke toegang Prio (Must / Should / Could)

De fysieke toegangen tot de servers moet worden beperkt qua personen en voor een bepaalde periode. Deze zullen goedgekeurd worden door de verantwoordelijke voor de veiligheid en getraceerd worden in een logboek.

SEC023 Documentatie Prio (Must / Should / Could)

Alle documentatie met betrekking tot fysieke of systeembeveiliging wordt geclassificeerd als vertrouwelijk/geheim en opgeslagen in een goedgekeurde ruimte met beperkte toegang.

SEC024 Threat Model Prio (Must / Should / Could)

Het 'Threat Model'-proces moet worden gedefinieerd. Dit is het proces waarbij potentiële bedreigingen, zoals structurele kwetsbaarheden, kunnen worden geïdentificeerd, opgesomd en geprioriteerd vanuit het oogpunt van de hypothetische aanvaller. Met andere woorden, dit proces van het identificeren, tellen en prioriteren van potentiële bedreigingen weegt op een verdediger en zijn bedrijfsmiddelen (gegevens, systemen, enz.).

9.6 Vereisten buiten het toepassingsgebied

Out of Scope Requirements [OUT].

Een "vereiste buiten het toepassingsgebied" is een zakelijke, functionele, niet-functionele of technische eis waarmee geen rekening wordt gehouden als beperking voor de oplossing. Deze vereisten worden in deze sectie gemeld om te garanderen dat ze werden overwogen en geanalyseerd. Aan deze vereisten moet wel worden voldaan, maar dan buiten de oplossing zelf.

OUT001	Communicatie over de opening van het vooraf stemmen Geen oproepingsbrief, maar de inrichtende macht is verantwoordelijk voor de communicatie.
OUT002	Registratie voor Belgen die in het buitenland wonen Belgen die in het buitenland wonen en die willen stemmen, moeten zich registreren voor het hybride systeem. Ze moeten een PDF-formulier downloaden (dat niet gewijzigd kan worden) van de website van Buitenlandse Zaken en dit terugsturen. De burger ontvangt dan vervolgens per post of e-mail een uitnodiging met uitleg over deze nieuwe stemmethode (procedure).
OUT003	Hulp bij het invoeren van de stembiljetten Geen systeem om stembiljetten te scannen.
OUT004	Aangeven van de samenstelling van de ontvangst- en telbureaus Het hybride systeem maakt het niet mogelijk om leden van de ontvangst- en stemopnemingsbureaus in te voeren, nadat ze de eed hebben afgelegd: <ul style="list-style-type: none">- Datum van de verkiezingen- Kanton/kieskring/college (stemming Europees Parlement) electoraal- Nummer van het stemopnemingsbureau- Naam van de persoon- Rol (voorzitter, bijzitters of getuigen) Het hybride systeem staat niet toe dat er redenen worden gegeven voor een beoordelaar of voorzitter die weigert aanwezig te zijn op de tel/ontvangst kantoren. Het hybride systeem maakt het niet mogelijk om verzoeken en beslissingen over het al dan niet ontheffen van de beoordelaars of voorzitters die het verzoek hebben ingediend, te coderen (beslissingslogboeken).
OUT005	Invoeren van de telling van de stembiljetten Met het hybride systeem kunnen leden van de ontvangst- en stemopnemingsbureaus alleen het aantal stembiljetten per type invoeren, nadat ze de telling hebben gecontroleerd en voordat ze de stemmen invoeren: <ul style="list-style-type: none">- Geldige stembiljetten- Gevalideerde verdachte en betwiste stembiljetten- Geannuleerde verdachte en betwiste stembiljetten- Blanco of ongeldige stembiljetten- Geldig en gevalideerde stembiljetten die verworpen werden omdat kiezers in persoon hebben gestemd Verificatie van de tellingen: <ul style="list-style-type: none">- Aantal geldige stembiljetten = aantal ontvangen stembiljetten - aantal blanco of ongeldige stembiljetten - aantal geannuleerde verdachte en betwiste stembiljetten

-
- Aantal geldige stembiljetten = aantal geldige stembiljetten - aantal gevalideerde verdachte en betwiste stembiljetten
 - Aantal afgedrukte stembiljetten = aantal ontvangen stembiljetten + aantal verloren stembiljetten

OUT006 Handmatig invoeren van de stembiljetten

Het hybride systeem staat niet toe dat leden van het ontvangst- en stemopnemingsbureau de volgende informatie invoeren na het openen van de dubbele enveloppen en het controleren van de 'K'-verificatiecode:

- Datum
- Tijdstip
- Invoerder (bijzitter)
- 'K'-verificatiecode
- Stem
- Oorsprong van de stemmen
 - o Stem van Belgen in België
 - o Stem van Belgen in het buitenland
- Soorten stembiljetten
 - o Geldige stembiljetten
 - o Gevalideerde verdachte en betwiste stembiljetten
 - o Geannuleerde verdachte en betwiste stembiljetten
 - o Blanco of ongeldige stembiljetten

OUT007 Invoerinterface voor toegang tot de algemene stembeheermodule

Het hybride systeem bevat geen interface voor het invoeren van informatie in de algemene stembeheermodule.

De invoer gebeurt door de leden van de bureaus voor de volgende gegevens:

- Samenstelling van de ontvangst- en stemopnemingsbureaus
- Niet-aanwezigheid en weigering van opgeroepen burgers om deel te nemen aan de bureaus
- Telling van geherkwalificeerde stembiljetten per type
- Stemopneming

OUT008 Raadpleging van de stemmen door de belanghebbenden

De raadpleging in de algemene stembeheermodule is beperkt tot de leden van het stembureau.

OUT009 Valideren van de stemopnemingen

Het hybride systeem stelt de voorzitters niet in staat om de invoer van de stemmen door de bijzitters te valideren.

Door de handmatige telling van de stemmen voorafgaand aan de invoer te vergelijken met het aantal stemmen dat door de bijzitters is ingevoerd.

OUT010 Sluiting van de stemopneming

Het hybride systeem stelt de voorzitters van de ontvangst-/stemopnemingsbureaus niet in staat om het einde van de invoer en validatie van de stemmen te bekrachtigen door middel van een proces-verbaal. Dit wordt voorzien in een andere verkiezingsbeheermodule of wordt met de hand opgemaakt.

OUT011 Opstellen van de processen-verbaal en de ontvangstbewijzen

Met het hybride systeem kunnen de processen-verbaal die door de verschillende ontvangst-/stemopnemingsbureaus worden uitgegeven, niet worden gegenereerd, gepubliceerd en geregistreerd.

- Proces-verbaal van de eerste telling van de stembiljetten per soort:
 - o Geldige stembiljetten
 - o Gevalideerde verdachte stembiljetten
 - o Geannuleerde verdachte stembiljetten
 - o Blanco of ongeldige stembiljetten
- Proces-verbaal van samenstelling van de ontvangst- en stemopnemingsbureaus:
 - o Datum van de verkiezingen
 - o Kanton/kieskring
 - o Nummer van het bureau
- Ontvangstbewijzen voor dubbele omslagen die per post worden bezorgd:
 - o Datum
 - o Aantal dubbele omslagen
 - o Nummer van het bureau
- Proces-verbaal van stemopneming
 - o Aantal zetels per partij
 - o Gekozen kandidaten in elke partij

Dit is voorzien in de andere beheermodules voor de verkiezingen.

OUT012 Rapporten en dashboards

Het hybride systeem laat niet toe om rapporten te produceren op basis van verzoeken van belanghebbenden.

Deze rapporten moeten gemakkelijk toegankelijk zijn en selfservice bevorderen.

Deze rapporten en dashboards moeten ook automatisch worden bijgewerkt wanneer de gegevens worden bijgewerkt.

OUT013 Online ondersteuning voor de kiezers

Het hybride systeem voorziet geen eerstelijns ondersteuning, een ondersteuning voor burgers die willen stemmen.

Het hybride systeem voorziet niet in de creatie van een documentatiegids die toegankelijk is in het systeem, link naar een hotline, helpdesk, implementatie van een ChatBox, enz.

OUT014 Consolidatie van de kiezerslijsten

Het hybride systeem voorziet niet in de integratie van de kiezerslijsten in België en de lijsten van Belgische kiezers in het buitenland.

OUT015 Beheer van het stemmen bij volmacht

Het hybride systeem voorziet niet in het beheer van het stemmen bij volmacht.

Kiezers kunnen hun stem uitbrengen door een volmacht te geven aan een andere kiezer (artikel 147bis van het Kieswetboek). Op deze manier kan de gevolmachtigde namens de volmachtgever stemmen.

Voortaan is het mogelijk om een volmacht te geven aan een andere kiezer. Een kiezer mag slechts één volmacht hebben. Volmachten kunnen worden gegeven tot de dag van de verkiezingen in de gevallen 1 tot 6 hieronder, en tot de dag voor de dag van de verkiezingen als je op vakantie bent in het buitenland (geval nr. 7).

OUT016 Bezorging van de gegevens

Het hybride systeem voorziet niet in het verzenden van de inhoud van post naar kiezers in België of in het buitenland naar postbeheerapplicaties.

OUT017 Opstellen en versturen van de oproepingsbrieven

- Voor Belgische kiezers die in België stemmen: uitnodigingen per post.
 - Voor Belgische kiezers die in het buitenland stemmen: uitnodiging per post + toelichtende brief.
-

10 Oplossing

Deze sectie beschrijft het architectuurontwerp van het hybride systeem.

Ter herinnering, het TOGAF raamwerk en de Archimate-modelleertaal worden gebruikt:

1- De **businesslaag** betreft de bedrijfsprocessen, diensten, functies en gebeurtenissen van de bedrijfsentiteiten. Deze laag biedt producten en diensten aan klanten, die worden gerealiseerd door bedrijfsprocessen die worden uitgevoerd door de verschillende bedrijfsactoren en -rollen.

2- De **toepassingslaag** betreft de softwaretoepassingen die de onderdelen van het bedrijf en de organisatie ondersteunen met applicatiediensten.

3- De **technologielaag** betreft de hardware- en communicatie-infrastructuur om de applicatielaag te ondersteunen. Deze laag levert de infrastructuurdiensten die nodig zijn om de applicaties uit te voeren, geïmplementeerd door de computer- en communicatiehardware en de systeemsoftware.

10.1 Motivatiediagram

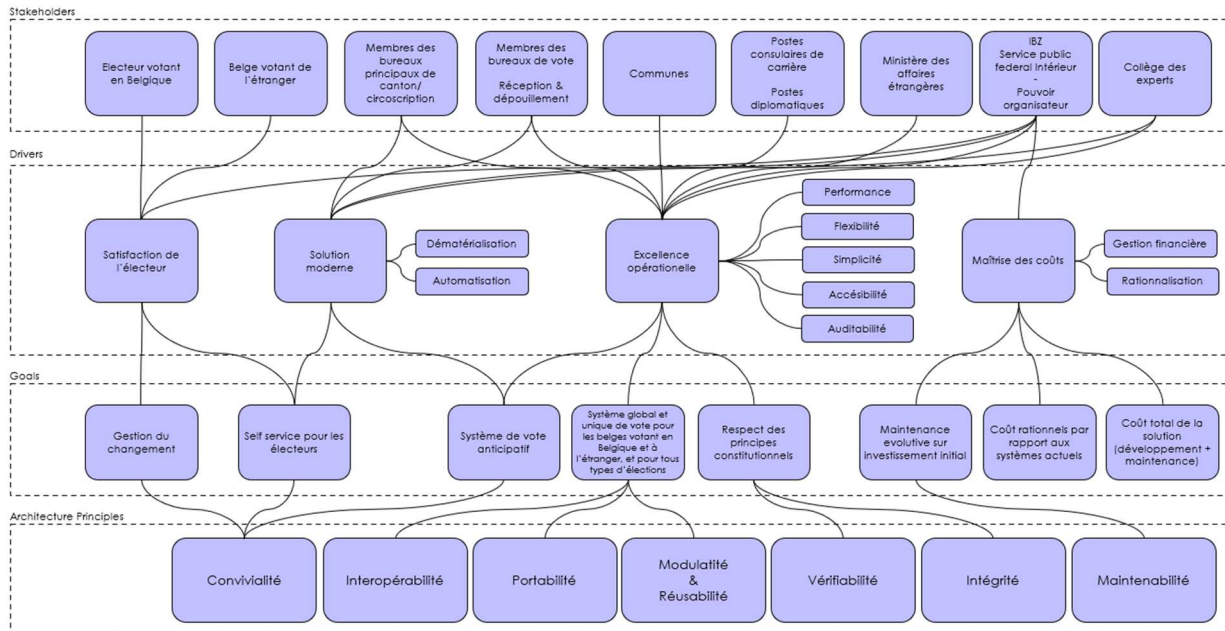
De motivatie behandelt de manier waarop de bedrijfsarchitectuur is afgestemd op de context ten tijde van het ontwerp.

Het motivatiediagram wordt gebruikt om het waarom, de redenen en de motivaties te modelleren die het ontwerp van de bedrijfsarchitectuur hebben geleid en beperkt. Het presenteert alle motivationele elementen, d.w.z. de elementen die de context en de onderliggende motieven leveren. De motivationele elementen werpen licht op de gemaakte ontwerpkeuzes, waardoor we de gemaakte keuzes in een veranderende context kunnen begrijpen.

Het doel van dit diagram is om een volledig of gedeeltelijk overzicht te geven van het motivatieaspect door verschillende elementen met elkaar in verband te brengen:

- **STAKEHOLDERS.** De internationale norm met richtlijnen voor maatschappelijke verantwoordelijkheid, bekend als ISO 26000, definieert een stakeholder als "een individu of groep die een belang heeft bij een beslissing of activiteit van een organisatie".
- **DRIVERS.** Een driver is een externe of interne omstandigheid die een organisatie motiveert om haar doelstellingen te definiëren en de veranderingen door te voeren die nodig zijn om ze te bereiken.
- **GOAL.** Een "Goal" of doel vertegenwoordigt een intentieverklaring op hoog niveau, een gewenste richting of eindtoestand voor een organisatie en haar belanghebbenden.

- **ARCHITECTURE PRINCIPLE.** Een principe vertegenwoordigt een kwalitatieve intentieverklaring waaraan de architectuur moet voldoen.



Stakeholders	Stakeholders
Electeur votant en Belgique	Kiezer die in België stemt
Belge votant de l'étranger	Belg die vanuit het buitenland stemt
Membres des bureaux principaux de canton/circoscription	Leden van de hoofdbureaus van het kanton/de kieskring
Membres des bureaux de vote	Leden van de stembureaus
Réception & dépouillement	Ontvangst en stemopneming
Communes	Gemeenten
Postes consulaires de carrière	Beroepsconsulaire posten
Postes diplomatiques	Diplomatieke posten
Ministère des affaires étrangères	Ministerie van Buitenlandse Zaken
IBZ Service public federal Intérieur - Pouvoir organisateur	IBZ Federale Overheidsdienst Binnenlandse Zaken - Inrichtende macht
Collège des experts	College van Deskundigen
Drivers	Drivers
Satisfaction de l'électeur	Tevredenheid van de kiezer
Solution moderne	Moderne oplossing
Dématérialisation	Dematerialisering
Automatisation	Automatisering
Excelence opérationnelle	Operationele uitmuntendheid
Performance	Prestatie
Flexibilité	Flexibiliteit
Simplicité	Eenvoud
Accésibilité	Toegankelijkheid
Auditabilité	Controleerbaarheid

Maîtrise des coûts	Kostenbeheersing
Gestion financière	Financieel beheer
Rationalisation	Rationalisering
Goals	Doelen
Gestion du changement	Beheer van wijzigingen
Self service pour les électeurs	Zelfbediening voor kiezers
Système de vote anticipatif	Systeem om vooraf te stemmen
Système global et unique de vote pour les belges votant en Belgique et à l'étranger, et pour tous types d'élections	Globaal en uniek stelsysteem voor Belgen die stemmen in België en in het buitenland, en voor alle soorten verkiezingen
Respect des principes constitutionnels	Naleving van de Belgische grondwettelijke principes
Maintenance évolutive sur investissement initial	Evolutief onderhoud op initiële investering
Coût rationnels par rapport aux systèmes actuels	Rationele kosten in vergelijking met huidige systemen
Coût total de la solution (développement + maintenance)	Totale kostprijs van de oplossing (ontwikkeling + onderhoud)
Architecture Principles	Architectuurprincipes
Convivialité	Gebruiksvriendelijkheid
Interopérabilité	Interoperabiliteit
Portabilité	Overdraagbaarheid
Modularité & Réusabilité	Modulariteit en herbruikbaarheid
Vérifiabilité	Controleerbaarheid
Intégrité	Integriteit
Maintenabilité	Onderhoudbaarheid

Drivers:

- TEVREDENHEID van de kiezer: in een context waarin meerdere stelsystemen beschikbaar zijn voor de kiezer, moet het hybride systeem een positieve gebruikerservaring bieden, anders zal de kiezer zich wenden tot de andere systemen.
- MODERNE OPLOSSING: In een context waarin het verbruik van natuurlijke hulpbronnen wordt gerationaliseerd en digitalisering zich uitbreidt naar alle activiteiten in onze samenlevingen, is hybride stemmen een eerste stap in de richting van een volledig digitaal systeem. De automatisering van stemprocessen maakt deel uit van dit rationaliseringsproces en wordt mogelijk gemaakt door de digitalisering van stemmedia.
- OPERATIONELE UITMUNTENDHEID: De organiserende autoriteit heeft haar wens geuit om de stemoperaties te verbeteren: meer flexibiliteit, eenvoudigere processen, betere toegang tot stemapparatuur en meer controleerbaarheid om transparantie en democratische controle te garanderen.

- KOSTENBEHEERSING: Rationalisatie maakt het mogelijk om de beste oplossing te vinden, in overeenstemming met de vereisten, in verhouding tot de gedane investering, door het toepassen van de beste praktijken in financieel beheer en kostenbeheersing.

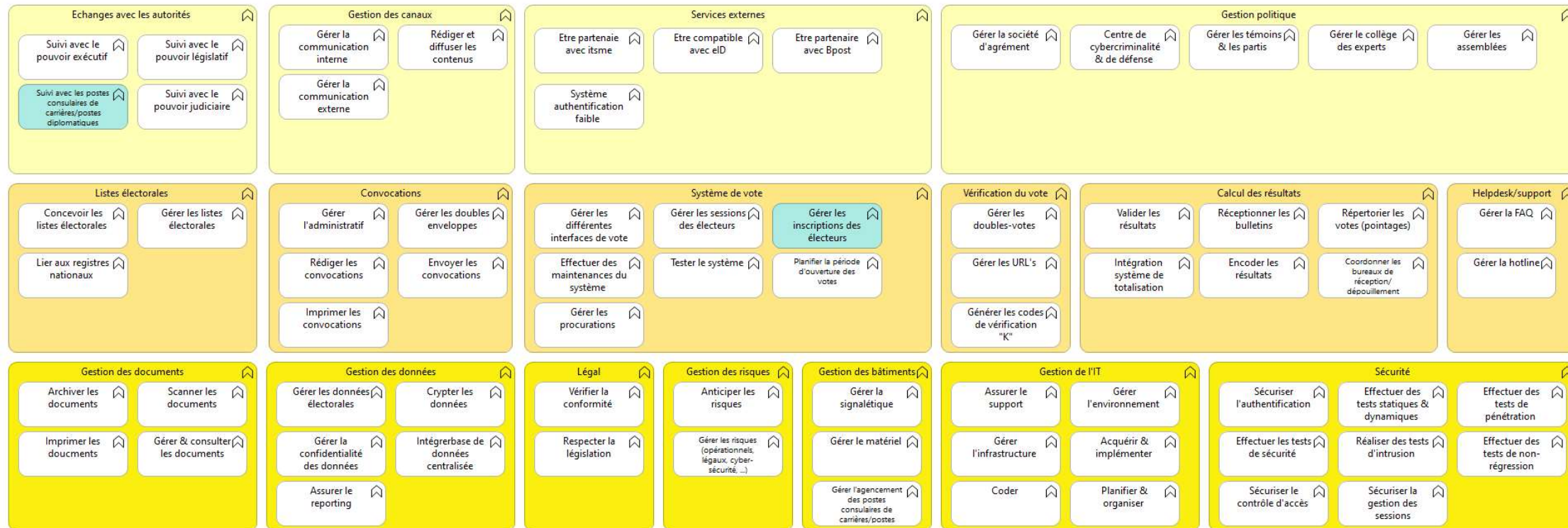
Goals:

- VERANDERINGSBEHEER: Essentieel element voor het succes van de oplossing. Een perfecte oplossing is een mislukking als ze niet wordt gebruikt. Dit betekent niet alleen communiceren, inspireren en opleiden van burgers, maar ook van belanghebbenden zoals lokale autoriteiten, leden van het kiesbureau, enz.
- SELF-SERVICE voor kiezers: Ervoor zorgen dat kiezers meer betrokken zijn bij het democratische leven van hun samenleving en in een vroeger stadium deelnemen aan het stemproces. Dit vergroot het vertrouwen van de burgers in het stemmechanisme. Het ontlast ook de inrichtende macht van een aantal taken door delegatie aan de kiezers.
- ANTICIPATIEF STEMSYSTEEM: De stemperiode van het hybride systeem voor het stemmen in België is niet beperkt tot de dag van de stemming. Dit stelt burgers in staat zich te organiseren om te kunnen stemmen en is een factor in de strijd tegen de dalende opkomst van burgers die gaan stemmen.
- GLOBAAL EN UNIEK SYSTEEM: Het hybride systeem moet zowel kiezers in België als Belgen in het buitenland bereiken. Het hybride systeem moet de Europese, federale en regionale verkiezingen dekken. Eén enkel systeem zal niet alleen zorgen voor meer consistentie en operationele controle, maar ook voor een betere gebruikerservaring en financiële controle.
- RESPECT VOOR CONSTITUTIONELE PRINCIPES: Dit zijn sine qua non voorwaarden, fundamentele beperkingen, zonder welke het hybride systeem niet kan worden geïmplementeerd.
- EVOLUTIEF ONDERHOUD: De investering in het hybride systeem wordt gerechtvaardigd door het feit dat het open is. Elke nieuwe functionaliteit moet worden geïmplementeerd op het hybride systeem zonder de oplossing volledig te herzien. Dit garandeert het rationele karakter van de investering: initiële investering voor een operationeel systeem, en indien nodig, verdere investering voor bijkomende functionaliteiten.
- RATIONELE KOSTEN vergeleken met die van huidige systemen: Met het oog op het rationaliseren van de kosten moet het hybride systeem een financieel voordeel bieden en een lagere Total Cost of Ownership (TCO) hebben dan de huidige systemen.
- TOTALE KOSTPRIJS van de oplossing: $TCO = CAPEX + OPEX$. Het gaat hier om de globale kostprijs van het systeem, bestaande uit de initiële investering voor het ontwikkelen, testen en implementeren van het systeem (CAPEX), evenals de operationele kosten over meerdere jaren (OPEX).

Architectuurprincipes:

- GEBRUIKSVRIENDELIJKHEID: De oplossing moet bruikbaar zijn voor burgers die geen specifieke opleiding hebben genoten.
- INTEROPERABILITEIT: De oplossing moet verbinding kunnen maken met andere systemen en modules om gegevens uit te wisselen (algemene stembeheermodule, stemmentellingmodule en hulpmodule voor het tellen van stemmen).
- OVERDRAAGBAARHEID: *Vendor Locking* en *Technology Locking* moeten vermeden worden. De oplossing, de software, moet op verschillende platformen en machines kunnen draaien.
- MODULARITEIT & HERBRUIKBAARHEID: De oplossing is een module die moet integreren met andere applicatiemodules. Het systeem moet kunnen worden hergebruikt in:
 - o Een versie-upgrade van de oplossing (identiek functioneel bereik)
 - o Een functionele evolutie van de oplossing (bijvoorbeeld het backendsysteem worden voor stemmen op papier)
- CONTROLEERBAARHEID: Het systeem moet betrouwbaar zijn (in termen van beveiligingsbeheer en correcte afhandeling van operationele problemen) en deze betrouwbaarheid moet worden beoordeeld.
- INTEGRITEIT: De oplossing moet zeer veilig zijn, met een sterke controle over de toegang tot functies en gegevens.
- HANDHAAFBAARHEID: Het moet mogelijk zijn om de oplossing te corrigeren en aan te passen als onderdeel van een continu verbeteringsproces. Dit principe garandeert een zekere mate van efficiëntie in de kostenbeheersing.

10.2 Bedrijfsarchitectuur (BusinessLayer)



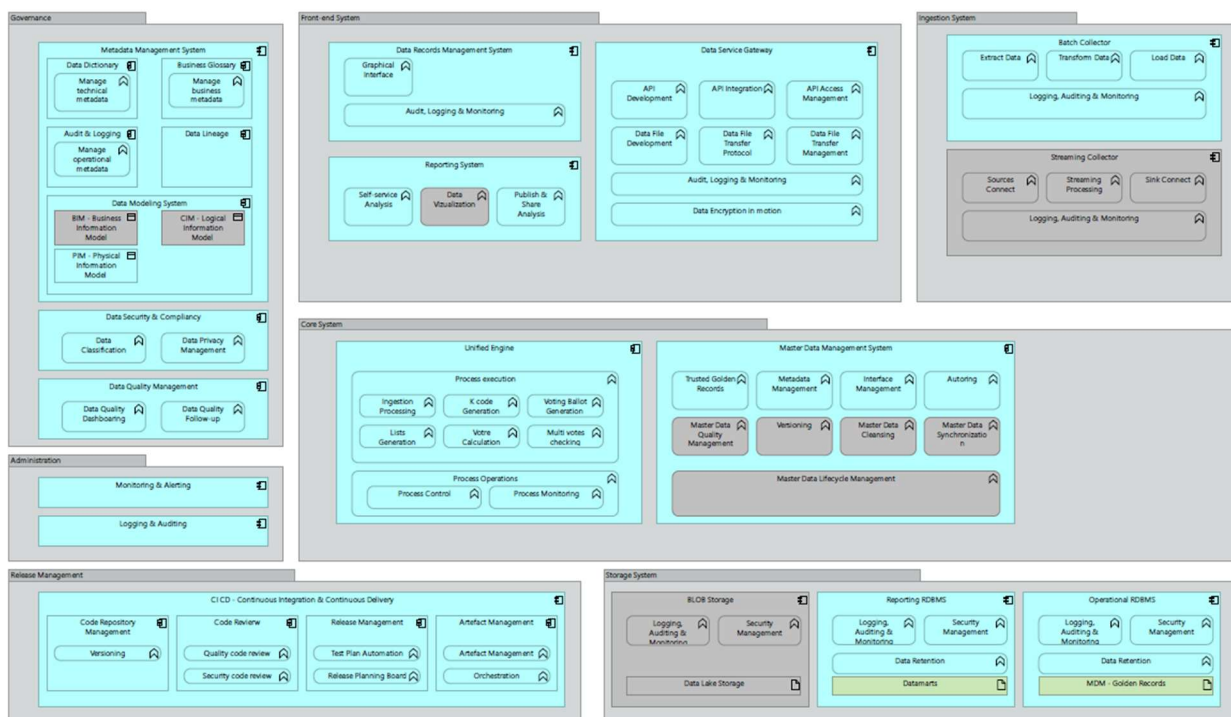
Echanges avec les autorités	Uitwisselingen met de autoriteiten
Suivi avec le pouvoir exécutif	Opvolging met de uitvoerende macht
Suivi avec les postes consulaires de carrières/postes diplomatiques	Opvolging met de beroepsconsulaire posten/diplomatieke posten
Suivi avec le pouvoir législatif	Opvolging met de wetgevende macht
Suivi avec le pouvoir judiciaire	Opvolging met de rechterlijke macht
Listes électorales	Kieslijsten
Concevoir les listes électorales	Opstellen van de kieslijsten
Lier aux registres nationaux	Koppelen aan de rijksregisters
Gérer les listes électorales	Beheren van de kieslijsten
Gestion des documents	Beheer van de documenten
Archiver les documents	Archiveren van de documenten
Imprimer les documents	Afdrukken van de documenten
Scanner les documents	Scannen van de documenten
Gérer & consulter les documents	Beheren en raadplegen van de documenten
Gestion des canaux	Beheer van de kanalen
Gérer la communication interne	Beheren van de interne communicatie
Gérer la communication externe	Beheren van de externe communicatie
Rédiger et diffuser les contenus	Opstellen en verspreiden van de inhoud
Convocations	Oproepingsbrieven
Gérer l'administratif	Beheren van de administratie
Rédiger les convocations	Opstellen van de oproepingsbrieven
Imprimer les convocations	Afdrukken van de oproepingsbrieven
Gérer les doubles enveloppes	Beheren van de dubbele omslagen
Envoyer les convocations	Versturen van de oproepingsbrieven
Gestion des données	Gegevensbeheer
Gérer les données électorales	Beheren van de verkiezingsgegevens
Gérer la confidentialité des données	Beheren van de vertrouwelijkheid van de gegevens
Assurer le reporting	Verzekeren van de rapportering
Crypter les données	Versleutelen van de gegevens
Intégrer base de données centralisée	Integreren van de gecentraliseerde gegevens
Services externes	Externe diensten
Etre partenaire avec itsme	Samenwerken met itsme
Système authentification faible	Zwak verificatiesysteem
Etre compatible avec eID	Compatibel zijn met eID
Etre partenaire avec Bpost	Samenwerken met bpost
Système de vote	Stemsysteem
Gérer les différentes interfaces de vote	Beheren van de verschillende steminterfaces
Effectuer des maintenances du système	Uitvoeren van het systeemonderhoud
Gérer les procurations	Beheren van de volmachten
Gérer les sessions des électeurs	Beheren van de kiezerssessies
Tester le système	Testen van het systeem
Gérer les inscriptions des électeurs	Beheren van de kiezersregistraties
Planifier la période d'ouverture des votes	Plannen van de periode van openstelling van de stemming
Légal	Wettelijk

Vérifier la conformité	Controleren van de conformiteit
Respecter la législation	Naleven van de wetgeving
Gestion des risques	Risicobeheer
Anticiper les risques	Anticiperen op risico's
Gérer les risques (opérationnels, légaux, cyber-sécurité, ...)	Beheren van de risico's (operationeel, juridisch, cybersecurity, enz.)
Gestion des bâtiments	Beheer van de gebouwen
Gérer la signalétique	Beheren van de bewegwijzering
Gérer le matériel	Beheren van het materieel
Gérer l'agencement des postes consulaires de carrières/postes	Beheren van de indeling van de beroepsconsulaire posten/posten
Gestion politique	Politiek beheer
Gérer la société d'agrément	Beheren van de accreditatieorganisatie
Centre de cybercriminalité & de défense	Cybercriminaliteits- en defensiecentrum
Gérer les témoins & les partis	Beheren van de getuigen en de partijen
Gérer le collège des experts	Beheren van het College van Deskundigen
Gérer les assemblées	Beheren van de parlementen
Vérification du vote	Verificatie van de stemming
Gérer les doubles-votes	Beheren van de dubbele stemmen
Gérer les URL's	Beheren van de URL's
Générer les codes de vérification "K"	Genereren van de 'K'-verificatiecodes
Calcul des résultats	Berekening van de resultaten
Valider les résultats	Valideren van de resultaten
Intégration système de totalisation	Integratie totaliseringssysteem
Réceptionner les bulletins	Ontvangen van de stembiljetten
Encoder les résultats	Invoeren van de resultaten
Répertorier les votes (pointages)	Inventariseren van de stemmen (aanstippen)
Coordonner les bureaux de réception/dépouillement	Coördineren van de ontvangst-/stemopnemingsbureaus
Helpdesk/support	Helpdesk/support
Gérer la FAQ	Beheren van de FAQ's
Gérer la hotline	Beheren van de hotline
Gestion de l'IT	Beheer van de IT
Assurer le support	Verzekeren van de ondersteuning
Gérer l'infrastructure	Beheren van de infrastructuur
Coder	Invoeren
Gérer l'environnement	Beheren van de omgeving
Acquérir & implémenter	Verwerven en implementeren
Planifier & organiser	Plannen en organiseren
Sécurité	Veiligheid
Sécuriser l'authentification	Beveiligen van de authenticatie
Effectuer les tests de sécurité	Uitvoeren van de veiligheidstests
Sécuriser le contrôle d'accès	Beveiligen van de toegangscontrole
Effectuer des tests statiques & dynamiques	Uitvoeren van de statische en dynamische tests
Réaliser des tests d'intrusion	Uitvoeren van de inbraaktests
Sécuriser la gestion des sessions	Beveiligen van het beheer van de sessies
Effectuer des tests de pénétration	Uitvoeren van de penetratietests

10.3 Functionele toepassingsarchitectuur (Application Layer)

De bedrijfsarchitectuur wordt gedefinieerd en de functionele vereisten worden gevalideerd. De toepassingsmodellen moeten worden geïdentificeerd door de referentiearchitectuur voor de applicatie te selecteren. Deze toepassingsmodellen moeten voldoen aan de vereisten en de bedrijfsarchitectuur ondersteunen.

De toepassingsarchitectuur is gebaseerd op de elementen van de Archimate-applicatie, een gemeenschappelijke taal die door architecten wordt gebruikt om de verschillende visies op de architectuur weer te geven. De volledige lijst en een korte uitleg van elk Archimate-applicatie-element werd toegevoegd als bijlage.



Sommige applicaties zullen absoluut geïmplementeerd moeten worden in de oplossing.

- **MUST** = De oplossing kan niet functioneel zijn zonder dat de toepassing is geïmplementeerd. MVP (Minimum Viable Product).
- **SHOULD** = De oplossing kan functioneel zijn in een eerste versie zonder dat de toepassing wordt geïmplementeerd, zolang de toepassing wordt opgenomen in een toekomstige versie.
- **COULD** = Dit is een "nice to have", het niet implementeren van deze toepassing is geen blokkerend punt voor de aanvaarding.

Governance

Voor het governance-gedeelte hebben we applicaties nodig om het volgende te handhaven:

- Gegevenswoordenboek
 - **MUST**
 - Aangezien het systeem gegevens moet beheren met een specifieke classificatie (bijv. vertrouwelijkheid) en ook informatie moet produceren voor belanghebbenden, is het essentieel om een middel te hebben om deze gegevens op een optimale manier te verzamelen en te onderhouden. Het gegevenswoordenboek wordt gebruikt om de structuur en inhoud van de gegevens te catalogiseren en te communiceren, en biedt zinvolle beschrijvingen voor afzonderlijk benoemde gegevensobjecten.
- Bedrijfswoordenlijst
 - **MUST**
 - Naast het gegevenswoordenboek kan het beheer van bedrijfstermen worden vergemakkelijkt door een bedrijfswoordenlijst. Ter herinnering: het gegevenswoordenboek beschrijft technische metadata en de bedrijfswoordenlijst beheert bedrijfsmetadata. Dus, om hetzelfde zakelijke begrip van de gegevens te hebben en de link te leggen tussen het bedrijfsconcept en de verschillende representaties ervan in de technische gegevens, kan de bedrijfswoordenlijst deze leemte opvullen. In een perfecte wereld komt de semantische laag die wordt toegepast op de belanghebbenden van de gegevens uit de bedrijfswoordenlijst.
- Data Lineage
 - **MUST**
 - Het is verplicht om het door de gegevens afgelegde traject te kennen, van het punt van binnenkomst tot de verschillende toepassingen ervan. Dit maakt het ook mogelijk om impactanalyses uit te voeren in het geval van een verandering in de gegevensbron.
- Audit & Logging
 - **MUST**
 - Nodig om te voldoen aan de beveiligingsvereisten in verband met de stemming.
- Systeem voor gegevensmodellering
 - **MUST**
 - Dit moet de functionele en technische analyse ondersteunen door conceptuele, logische en fysieke datamodellen op één plaats te creëren en gemakkelijk met iedereen te delen.
- Beheer van de gegevenskwaliteit
 - **SHOULD**

- De kwaliteit van de gegevens moet beheerd worden op bronniveau. Maar als we betrouwbare informatie voor processen en rapporten willen hebben, moeten kwaliteitsindicatoren beschikbaar zijn voor zakelijke eindgebruikers.

Frontendsystemen

Voor het frontendsysteem dat we uiteenzetten aan de eindgebruikers, hebben we voornamelijk de volgende elementen nodig:

- Rapportagesysteem
 - **MUST**
 - De 'Business Intelligence'-platformen (BI) bieden mogelijkheden in drie categorieën:
 - Analyse, zoals online analytische verwerking (OLAP) en de zelfbedieningselementen;
 - Informatieverspreiding, zoals rapporten en dashboards;
 - Visualisatie van gegevens.

Invoersysteem

Hoe worden gegevens vanuit externe bronnen in het systeem ingevoerd? Het invoersysteem komt hieraan tegemoet door het volgende mogelijk te maken:

- Batchverzamelaar
 - **MUST**
 - Het invoermechanisme zal hoofdzakelijk batchgeoriënteerd zijn, waarbij de batchverzamelaar over het algemeen snapshots of delta's vanuit bronsystemen verzamelt. Dit zal de rol zijn van de ETL-applicatie.

Opslagsysteem

De gegevens (bronnen en doelen) zullen voornamelijk worden opgeslagen in de vorm van:

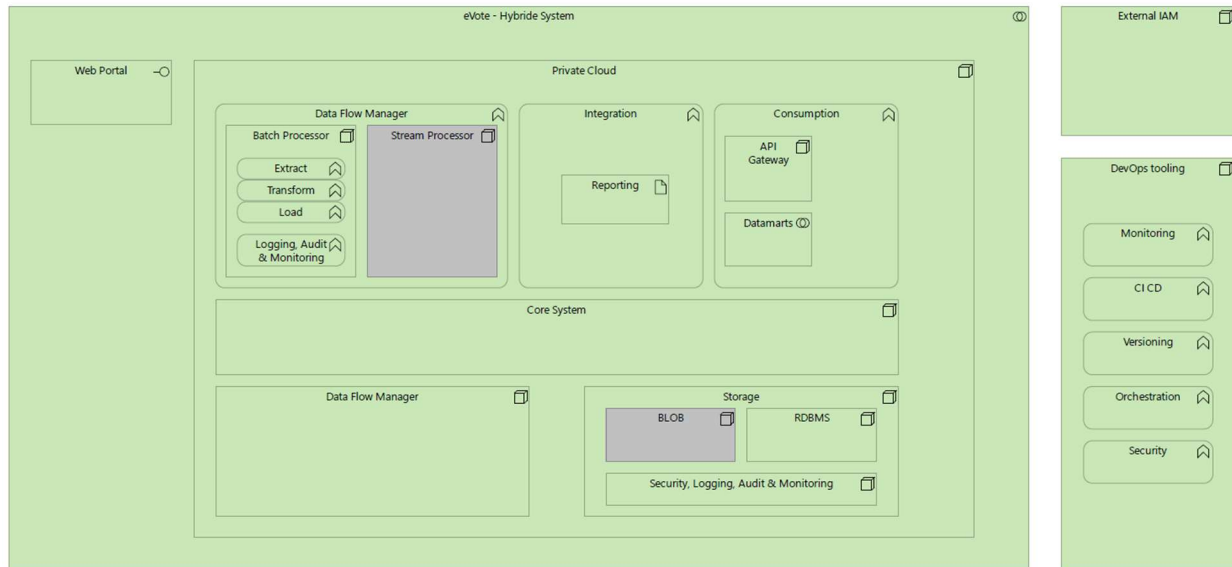
- Bestandsopslag
 - **MUST**
 - Deze opslag wordt voornamelijk gebruikt om RAW-gegevens op te slaan die in batches (via het batchverzamelprogramma) uit bronsystemen worden binnengehaald en opgeslagen voor verdere verwerking en transformatie.
- Reporting RDBMS
 - **MUST**
 - Noodzaak van een gedistribueerd datawarehousesysteem dat fouttolerant is en het verrichten van analyses mogelijk maakt. Ter herinnering: een datawarehouse biedt een centrale opslagplaats van informatie die eenvoudig kan worden geanalyseerd om rapporten en dashboards te creëren.

Release Management

Dit onderdeel gaat voornamelijk over de manier waarop we de 'continue integratie'- en 'continue levering'-functionaliteiten gaan implementeren, ook wel bekend als het DEVOPS-gedeelte.

- Code Repository Management
 - **MUST**
 - Dit onderdeel betreft de continue integratie van nieuwe stukken code die gegevensverwerking en transformaties vertegenwoordigen. Het beheert de verschillende versies van de code en de manier waarop deze worden geïntegreerd in het programma als geheel.
- Artefact Repository
 - **SHOULD**
 - Met een Artefact Repository kan je Release Pipeline geversioneerde artefacten en hun afhankelijkheden publiceren en ophalen met behulp van centrale referentiekaders die toegankelijk zijn vanuit andere omgevingen. Het artefact kan bestaan uit project broncode, afhankelijkheden, binaries of resources, en kan in verschillende vormen worden weergegeven afhankelijk van de technologie.
- Release Management
 - **MUST**
 - We hebben een applicatie nodig voor Release Management. Met toegang tot de Artefact Repository consumeert een Release Pipeline de artefacten en voert vervolgcacties uit binnen een multi-environment platform.

10.4 Technische architectuur (Technology Layer)



10.5 SWOT



Au lancement d'un produit ou d'un service, une analyse **SWOT** (**s**trenghts, **w**eaknesses, **o**pportunities, **t**hreats) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.

Dans notre cas, cette analyse nous permet de comparer les trois systèmes et de les analyser avec plus de recul.



SWOT	SWOT
Au lancement d'un produit ou d'un service, une analyse SWOT (strenghts , weaknesses , opportunities , threats) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.	Wanneer een product of een dienst gelanceerd wordt, geeft een SWOT -analyse (' Strenghts ' (sterktes), ' Weaknesses ' (zwaktes), ' Opportunities ' (kansen), ' Threats ' (bedreigingen)) aan op welke sterktes en kansen kan worden voortgebouwd, maar ook met welke bedreigingen en zwaktes rekening moet worden gehouden.
Dans notre cas, cette analyse nous permet de comparer les trois systèmes et de les analyser avec plus de recul.	In ons geval stelt deze analyse ons in staat om de drie systemen te vergelijken en vanuit een breder perspectief te analyseren.
S	S
Forces	Sterktes
W	W
Faiblesses	Zwaktes
O	O
Opportunités	Kansen
T	T
Menaces	Bedreigingen
Les forces & faiblesses sont des choses internes à l'organisation et sur lesquelles celle-ci a une marge de manoeuvre.	Sterktes en zwaktes zijn zaken die binnen de organisatie liggen en waarover de organisatie manoeuvreerruimte heeft.
Kansen en bedreigingen zijn zaken die buiten de organisatie liggen en waarover ze geen manoeuvreerruimte heeft.	Kansen en bedreigingen zijn zaken die buiten de organisatie liggen en waarover ze geen manoeuvreerruimte heeft.

10.5.1 SWOT Business



SYSTÈME HYBRIDE



Forces

- Mode de vote supplémentaire
- Amélioration du processus d'authentification
- Élargissement de la période de vote
- Meilleure accessibilité pour électeurs à mobilité réduite ou ne sachant pas se déplacer
- Possibilité de voter depuis n'importe quel endroit et n'importe quand
- Rapidité du vote
- Suppression des coûts de déplacement pour l'électeur
- Fidélité du bulletin de vote (le bulletin expédié reflète l'intention de vote)
- Possibilité de vérifier que le vote est bien arrivé en Belgique
- Autorisation de re-voter dans un bureau en Belgique
- Diminution des coûts du pouvoir organisateur
- Augmentation du taux de participation
- Logistique réduite pour le pouvoir organisateur (pas d'isoloir, matériel...)
- Gain de temps pour l'électeur

Opportunités

- Modernisation des systèmes actuels, dématérialisation
- Promotion du système via une campagne nationale de publicité
- Promotion du système par les politiques
- Crise sanitaire, pandémie
- Accélération de la digitalisation
- Curiosité des électeurs

Faiblesses

- Absence de contrôle du scrutin par les citoyens
- Adaptation des règles à différents niveaux et du système électoral
- Augmentation du nombre de scrutins illisibles
- Contradiction avec la volonté de digitaliser le vote (impression papier du bulletin)
- Requiert un niveau de sécurité élevé
- Obligation de respecter les exigences légales
- Complexité d'implémentation et de gestion
- Mise en place d'une infrastructure IT non négligeable & sécurisée
- Coûts opérationnels à charge de l'administration publique
- Obligation de s'authentifier via méthode CSAM
- Impossibilité d'afficher l'ensemble des candidats/partis sur une unique face A4
- Nécessité pour les électeurs de disposer du matériel nécessaire (imprimante...)
- Coût d'envoi des bulletins à charge de l'électeur (impression, timbres, enveloppes...)
- Génération d'un code k pour la vérification du vote
- Difficulté de garantir la confidentialité & le secret du vote
- Risques de perte de courrier, retard d'expédition...
- Difficulté dans le suivi des bulletins de vote
- Lenteur dans le dépouillement des votes
- Risques d'erreurs humaines lors du pointage, dépouillement et encodage des résultats
- Risques d'usurpation d'identité, achat de vote et coercition
- Risques de fraude
- Fracture numérique ne permettant pas à certaines personnes d'accéder à ce type de système de vote

Menaces

- Opposition des partis politiques
- Dépendance avec les services postaux
- Risques d'attaques cyber-criminelles
- Risques de phishing (hameçonnage)
- Inquiétude quant au principe du vote libre et non contraint
- Coercition de l'électeur

SWOT	SWOT
SYSTÈME HYBRIDE	HYBRIDE SYSTEEM
Forces	Sterktes
Mode de vote supplémentaire	Extra stemmethode
Amélioration du processus d'authentification	Verbetering van het authenticatieproces
Elargissement de la période de vote	Verlenging van de stemperiode
Meilleure accessibilité pour électeurs à mobilité réduite ou ne sachant pas se déplacer	Verbeterde toegankelijkheid voor kiezers die minder mobiel zijn of zich niet kunnen verplaatsen
Possibilité de voter depuis n'importe quel endroit et n'importe quand	Mogelijkheid om overal en altijd te stemmen
Rapidité du vote	Snelheid van het stemmen
Suppression des coûts de déplacement pour l'électeur	Geen verplaatsingskosten meer voor de kiezer
Fidélité du bulletin de vote (le bulletin expédié reflète l'intention de vote)	Betrouwbaarheid van het stembiljet (het verstuurd stembiljet weerspiegelt de stemintentie)
Possibilité de vérifier que le vote est bien arrivé en Belgique	Mogelijkheid om te controleren of de stem in België is aangekomen
Autorisation de re-voter dans un bureau en Belgique	Toestemming om opnieuw te stemmen in een stembureau in België
Diminution des coûts du pouvoir organisateur	Vermindering van de kosten voor de inrichtende macht
Augmentation du taux de participation	Stijging van het opkomstpercentage
Logistique réduite pour le pouvoir organisateur (pas d'isoloir, matériel...)	Minder logistiek voor de inrichtende macht (geen stembokjes, apparatuur, enz.)
Gain de temps pour l'électeur	Tijdswinst voor de kiezer
Opportunités	Kansen
Modernisation des systèmes actuels, dématérialisation	Modernisering van huidige systemen, dematerialisatie
Promotion du système via une campagne nationale de publicité	Promotie van het systeem via een nationale reclamecampagne
Promotion du système par les politiques	Promotie van het systeem door politici
Crise sanitaire, pandémie	Gezondheids crisis, pandemie
Accélération de la digitalisation	Versnelde digitalisering
Curiosité des électeurs	Nieuwsgierigheid van de kiezers
Faiblesses	Zwaktes
Absence de contrôle du scrutin par les citoyens	Gebrek aan publiek toezicht op de stemmingsprocedure
Faiblesses	Zwaktes
Adaptation des règles à différents niveaux et du système électoral	Aanpassing van regels op verschillende niveaus en van het kiesstelsel
Contradiction avec la volonté de digitaliser le vote (impression papier du bulletin)	Tegenstrijdigheid met de wens om te digitaliseren (papieren stembiljetten)
Requiert un niveau de sécurité élevé	Vereist een hoog beveiligingsniveau
Obligation de respecter les exigences légales	Verplichting om te voldoen aan wettelijke vereisten

Complexité d'implémentation et de gestion	Complexiteit van implementatie en beheer
Mise en place d'une infrastructure IT non négligeable & sécurisée	Implementatie van een aanzienlijke en veilige IT-infrastructuur vereist
Coûts opérationnels à charge de l'administration publique	Operationele kosten te dragen door de overheid
Obligation de s'authentifier via méthode CSAM	Verplichting tot authenticatie via CSAM-methode
Impossibilité d'afficher l'ensemble des candidats/partis sur une unique face A4	Het is onmogelijk om alle kandidaten/partijen op één A4-kant weer te geven
Nécessité pour les électeurs de disposer du matériel nécessaire (imprimante...)	De kiezers moeten over de nodige apparatuur beschikken (printer, enz.)
Coût d'envoi des bulletins à charge de l'électeur (impression, timbres, enveloppes...)	De kosten voor het verzenden van de stembiljetten worden gedragen door de kiezer (afdrukken, postzegels, enveloppen, enz.)
Génération d'un code k pour la vérification du vote	Generatie van een k-code voor stemverificatie
Difficulté de garantir la confidentialité & le secret du vote	Moeilijkheid om de vertrouwelijkheid en geheimhouding van de stemming te garanderen
Risques de perte de courrier, retard d'expédition....	Risico's van verloren gegane post, vertragingen bij de verzending, enz.
Difficulté dans le suivi des bulletins de vote	Moeilijkheid om stembiljetten te traceren
Lenteur dans le dépouillement des votes	Vertragingen bij het tellen van de stemmen
Risques d'erreurs humaines lors du pointage, dépouillement et encodage des résultats	Risico's van menselijke fouten tijdens het tellen, stemopneming en invoer van de resultaten
Risques d'usurpation d'identité, achat de vote et coercition	Risico's van identiteitsdiefstal, kopen van stemmen en dwang
Risques de fraude	Risico's van fraude
Fracture numérique ne permettant pas à certaines personnes d'accéder à ce type de système de vote	Digitale kloof waardoor sommige mensen geen toegang hebben tot dit type stelsysteem
Menaces	Bedreigingen
Opposition des partis politiques	Tegenstand van politieke partijen
Dépendance avec les services postaux	Afhankelijkheid van postdiensten
Risques d'attaques cyber-criminelles	Risico's van cybercriminele aanvallen
Risques de phishing (hameçonnage)	Risico's van phishing
Inquiétude quant au principe du vote libre et non contraint	Ongerustheid over het principe van vrij en ongehinderd stemmen
Coercition de l'électeur	Dwang van de kiezer

10.5.2 Technische SWOT



SYSTÈME HYBRIDE

Forces

- Infrastructure sécurisée (private cloud)
- Data centers conformes aux normes : ISA 3402 type 2, ISO 9001, ISO 270001...
- Résilience en cas de catastrophe
- Processus d'authentification connu & rapide (CSAM)
- Double système d'authentification
- Possibilité d'utiliser la technologie appropriée à chaque solution grâce à l'architecture microservices
- Flexibilité de l'infrastructure permettant d'optimiser les ressources & coûts de chaque service en fonction des besoins
- Traçabilité des actions pour des audits
- Architecture futureproof (containers as a service CaaS)
- Architecture logicielle stateless (scalabilité)

Faiblesses

- Coûts d'hébergement et de maintenance (private cloud)
- Difficultés d'intégration avec d'autres outils
- Complexité & coûts de développement
- SLA élevé, avec une balance valeur ajoutée VS coût faible
- Possibilité de dysfonctionnement technique, entraînant des problèmes potentiels lors des élections
- Difficulté de migration de la plateforme private cloud vers une autre
- Pas de solution intégrant toutes les fonctionnalités requises pour voter
- Collaboration d'un tiers dans le processus de vote (Bpost)
- Solution partielle faisant appel à des processus manuels et d'autres solutions partielles en termes de fonctionnalités

Opportunités

- Innovation & progrès technologique
- Combinaison & intégration des systèmes actuels
- Possibilité de mettre en oeuvre des fonctionnalités avancées telles que le vote mobile...
- Collaboration avec des organismes de recherche pour améliorer en continu la sécurité du système
- Expansion potentielle du système de vote électronique vers d'autres domaines, tels que les élections d'organisations privées
- Évolution facile vers le vote 100% en ligne

Menaces

- Exposition sur Internet (préoccupation en matière de sécurité)
- Sensible aux pannes internet & électriques des utilisateurs/communes
- Absence de réglementation standard (locale, nationale et européenne), impact potentiel à l'avenir
- Nécessité de compétences technologiques avancées pour les développements et la maintenance de la plateforme
- Possibilité de bugs ou de vulnérabilités non détectées dans le système qui pourraient être exploitées par des acteurs malveillants
- Risques de piratage ou de manipulation des résultats électoraux

Technique	Technisch
SWOT	SWOT
SYSTÈME HYBRIDE	HYBRIDE SYSTEEM
Forces	Sterktes
Infrastructure sécurisée (private cloud)	Beveiligde infrastructuur (private cloud)
Data centers conformes aux normes: ISA 3402 type 2, ISO 9001, ISO 270001...	Datacenters die voldoen aan normen: ISA 3402 type 2, ISO 9001, ISO 270001, enz.
Résilience en cas de catastrophe	Veerkracht in geval van een ramp
Processus d'authentification connu & rapide (CSAM)	Bekend en snel authenticatieproces (CSAM)
Double système d'authentification	Dubbel authenticatiesysteem
Possibilité d'utiliser la technologie appropriée à chaque solution grâce à l'architecture microservices	Mogelijkheid om voor elke oplossing de juiste technologie te gebruiken dankzij de microservices-architectuur
Flexibilité de l'infrastructure permettant d'optimiser les ressources & coûts de chaque service en fonction des besoins	Flexibiliteit van de infrastructuur om de middelen en kosten van elke dienst te optimaliseren in functie van de behoeften
Traçabilité des actions pour des audits	Traceerbaarheid van de acties voor audits

Architecture futureproof (containers as a service CaaS)	Toekomstbestendige architectuur (containers als service CaaS)
Architecture logicielle stateless (scalabilité)	Stateless softwarearchitectuur (schaalbaarheid)
Opportunités	Kansen
Innovation & progrès technologique	Innovatie en technologische vooruitgang
Combinaison & intégration des systèmes actuels	Combinatie en integratie van de huidige systemen
Possibilité de mettre en oeuvre des fonctionnalités avancées telles que le vote mobile...	Mogelijkheid om geavanceerde functies te implementeren, zoals mobiel stemmen...
Collaboration avec des organismes de recherche pour améliorer en continu la sécurité du système	Samenwerking met onderzoeksinstituten om de veiligheid van het systeem continu te verbeteren
Expansion potentielle du système de vote électronique vers d'autres domaines, tels que les élections d'organisations privées	Potentiële uitbreiding van het e-votingsysteem naar andere domeinen, zoals verkiezingen voor particuliere organisaties
Évolution facile vers le vote 100% en ligne	Gemakkelijke evolutie naar 100% online stemmen
Faiblesses	Zwaktes
Coûts d'hébergement et de maintenance (private cloud)	Hosting- en onderhoudskosten (private cloud)
Difficultés d'intégration avec d'autres outils	Moeilijkheden met integratie met andere tools
Complexité & coûts de développement	Complexiteit en ontwikkelingskosten
SLA élevé, avec une balance valeur ajoutée VS coût faible	Hoge SLA, met een geringe toegevoegde waarde in vergelijking met de kosten
Possibilité de dysfonctionnement technique, entraînant des problèmes potentiels lors des élections	Mogelijkheid van technische storing, wat tot potentiële problemen tijdens de verkiezingen kan leiden
Difficulté de migration de la plateforme private cloud vers une autre	Moeilijkheid om van een 'private cloud'-platform naar een ander te migreren
Pas de solution intégrant toutes les fonctionnalités requises pour voter	Geen oplossing die alle functionaliteiten integreert die nodig zijn voor het stemmen
Collaboration d'un tiers dans le processus de vote (Bpost)	Betrokkenheid van een derde partij bij het stemproces (bpost)
Solution partielle faisant appel à des processus manuels et d'autres solutions partielles en termes de fonctionnalités	Gedeeltelijke oplossing met handmatige processen en andere gedeeltelijke oplossingen in termen van functionaliteiten
Menaces	Bedreigingen
Exposition sur Internet (préoccupation en matière de sécurité)	Blootstelling aan het internet (veiligheidsrisico's)
Sensible aux pannes internet & électriques des utilisateurs/communes	Gevoelig voor internetonderbrekingen en stroompannes van gebruikers/gemeenten
Absence de réglementation standard (locale, nationale et européenne), impact potentiel à l'avenir	Geen standaard regelgeving (lokaal, nationaal en Europees), potentiële impact in de toekomst
Nécessité de compétences technologiques avancées pour les développements et la maintenance de la plateforme	Behoeft aan geavanceerde technologische competenties om het platform te ontwikkelen en te onderhouden

Possibilité de bugs ou de vulnérabilités non détectées dans le système qui pourraient être exploitées par des acteurs malveillants	Mogelijkheid van bugs of onopgemerkte kwetsbaarheden in het systeem die kunnen worden uitgebuit door kwaadwillenden
Risques de piratage ou de manipulation des résultats électoraux	Risico's van hacking of manipulatie van verkiezingsresultaten

11 Bijlagen




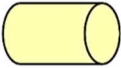
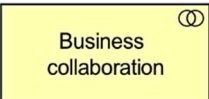




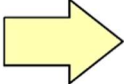





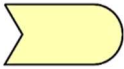
11.1 Glossarium


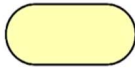
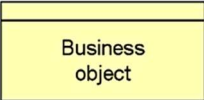

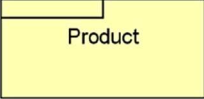
ID	Termijn	Definitie

11.2 Archimate-elementen

11.2.1 Business Architecture

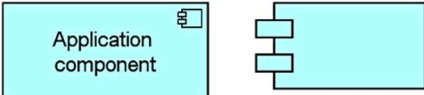

Tabel 1: Elementen van de 'Business'-laag






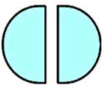

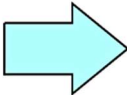




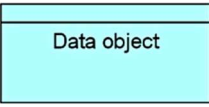
Item	Beschrijving	Notatie
Business Actor	Een businessentiteit die een gedrag kan uitvoeren.	 
Business Role	De verantwoordelijkheid voor het uitvoeren van een specifiek gedrag waaraan een actor kan worden toegewezen, of de rol die een actor speelt in een bepaalde actie of gebeurtenis.	 
Business Collaboration	Een samenvoeging van twee of meer elementen van de interne actieve structuur van de onderneming die samenwerken om een collectief gedrag uit te voeren.	 
Business Interface	Een toegangspunt waar een businessservice beschikbaar wordt gemaakt voor de omgeving.	 
Business Process	Een opeenvolging van businessgedragingen om een specifiek resultaat te bereiken, zoals een gedefinieerde reeks producten of diensten.	 
Business Function	Een reeks zakelijke gedragingen gebaseerd op een gekozen reeks criteria (meestal de vereiste middelen en/of professionele vaardigheden), nauw afgestemd op, maar niet noodzakelijk expliciet bestuurd door een organisatie.	 
Business Interaction	Een eenheid van collectief zakelijk gedrag uitgevoerd door (een samenwerking van) twee of meer zakelijke actoren, rollen of samenwerkingsverbanden.	 
Business Event	Een verandering in de toestand van de organisatie.	 

Item	Beschrijving	Notatie
Business Service	Het expliciet gedefinieerde gedrag dat een businessrol, businessactor of businesssamenwerking vertoont aan zijn omgeving.	
Business Object	Een concept dat in een bepaald activiteitsdomein wordt gebruikt.	
Contract	Een formele of informele specificatie van een overeenkomst tussen een leverancier en een consument die de rechten en plichten specificeert die verbonden zijn aan een product en die functionele en niet-functionele parameters voor interactie vastlegt.	
Representation	Een waarneembare vorm van de informatie die door een bedrijfsobject wordt overgebracht.	
Product	Een samenhangend geheel van diensten en/of passieve structurele elementen, vergezeld van een contract/set van overeenkomsten, dat als geheel wordt aangeboden aan klanten (intern of extern).	

11.2.2 Architecture Application

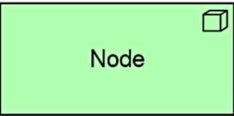
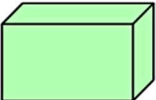
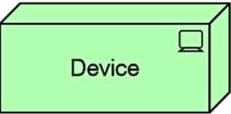
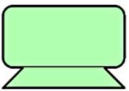
Tabel 2: Elementen van de 'Application'-laag

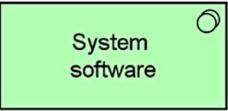
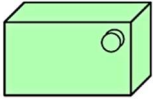
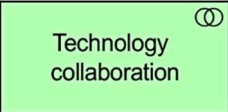
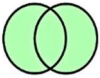

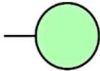

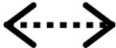

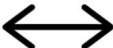



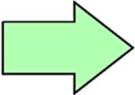

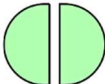
Item	Definitie	Notatie
Application Component	Een inkapseling van de applicatiefunctionaliteit afgestemd op de implementatiestructuur, die modulair en vervangbaar is.	
Application Collaboration	Een aggregaat van twee of meer elementen van de interne actieve structuur van de applicatie die samenwerken om collectief applicatiegedrag te bereiken.	


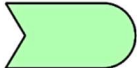

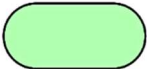
Item	Definitie	Notatie
Application Interface	Een toegangspunt waar applicatieservices beschikbaar worden gemaakt voor een gebruiker, een andere applicatiecomponent of een knooppunt.	 
Application Function	Het geautomatiseerde gedrag dat kan worden uitgevoerd door een applicatiecomponent.	 
Application Interaction	Een eenheid van collectief applicatiegedrag uitgevoerd door (een samenwerking van) twee of meer applicatiecomponenten.	 
Application Process	Een opeenvolging van applicatiegedragingen waarmee een specifiek resultaat wordt bereikt.	 
Application Event	Een toestandsverandering in de applicatie.	 
Application Service	Een expliciet gedefinieerd blootgesteld applicatiegedrag.	 
Data Object	Gestructureerde gegevens voor een geautomatiseerde verwerking.	

11.2.3 Architecture Technology

Tabel 3: Elementen van de 'Technology'-laag

Item	Definitie	Notatie
Node	Een computer of fysieke bron die andere computers of fysieke bronnen host, manipuleert of ermee interageert.	 
Device	Een fysieke computerbron waarop systeemsoftware en artefacten kunnen worden opgeslagen of ingezet voor uitvoering.	 

Item	Definitie	Notatie
System Software	Doelt op software die voorziet in of bijdraagt tot een omgeving voor de opslag, uitvoering en het gebruik van software of gegevens die in die omgeving worden ingezet.	 
Technology Collaboration	Een aggregaat van twee of meer elementen van de interne actieve structuur van de technologie die samenwerken om een collectief technologisch gedrag te bereiken.	 
Technology Interface	Een toegangspunt tot de technologiediensten die door een knooppunt worden aangeboden.	 
Path	Een verbinding tussen twee of meer knooppunten, waardoor deze knooppunten gegevens, energie of hardware kunnen uitwisselen.	 
Communication Network	Een verzameling structuren die knooppunten verbinden voor de transmissie, routing en ontvangst van gegevens.	 
Technology Function	Een reeks technologische gedragingen die door een knooppunt kunnen worden uitgevoerd.	 
Technology Process	Een opeenvolging van technologische gedragingen die kunnen worden gebruikt om een specifiek resultaat te behalen.	 
Technology Interaction	Een eenheid van collectief technologisch gedrag uitgevoerd door (een samenwerking van) twee of meer knooppunten.	 

Item	Definitie	Notatie
Technology Event	Een verandering van technologische toestand.	 
Technology Service	Een expliciet gedefinieerd blootgesteld technologiegedrag.	 
Artifact	Een gegevenselement dat wordt gebruikt of geproduceerd in een softwareontwikkelingsproces, of door de inzet en werking van een computersysteem.	